

[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

ManageWise® 2.6
Setup Guide



Novell®

ManageWise®
MANAGEMENT SOFTWARE

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without any obligation to notify any person or entity of such changes.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources. NetWare is a registered service mark of Novell, Inc.

Novell, NetWare, ManageWise, and LANalyzer are registered trademarks of Novell, Inc. in the United States and other countries.

The Novell Network Symbol, Client 32, HMI, Hub Management Interface, Internet Packet Exchange, IPX, IPX/SPX, LANtern, NetWare Management Agent, NCP, NetExplorer, NetWare 3, NetWare 4, NetWare 5, NetWare Client, NetWare Core Protocol, NetWare Connect, NetWare DOS Requester, NetWare Hub Services, NetWare Expert, NetWare IP, NetWare LANalyzer Agent, NetWare SFT III, Network Dashboard, NetWare Requester, NetWare Loadable Module, NLM, Novell Directory Services, Sequenced Packet Exchange, SMS, SPX, Virtual Loadable Module, and VLM are trademarks of Novell, Inc.

Copyright © 1993–98 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

**Novell, Inc.
2180 Fortune Drive
San Jose, CA 95131**

**ManageWise 2.6
Setup Guide
August 1998
100-003045-002D**

Apple, AppleLink, AppleTalk, LocalTalk, Macintosh, and Power Macintosh are registered trademarks and Apple Desktop Bus is a trademark of Apple Computer, Inc. ARCnet, is a registered trademark of Datapoint Corporation. Btrieve is a registered trademark of Pervasive Software, Inc. ARCserver, Cheyenne, and InocuLAN are registered trademarks of Cheyenne Software, a subsidiary of Computer Associates. CompuServe is a registered trademark of CompuServe Incorporated. DECnet is a trademark of Digital Equipment Corporation. AST is a registered trademark of AST Research, Inc. NetPort and SatisFAXtion are registered trademarks and StorageExpress is a trademark of Intel Corporation. IBM, OS/2, PC/AT, and PS/2 are registered trademarks and PC/XT is a trademark of International Business Machines Corporation. Hayes is a registered trademark of Hayes Microcomputer Products, Inc. LANSpool is a registered trademark of LAN Systems, Inc. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks and Windows 95 is a trademark of Microsoft Corporation. QEMM is a registered trademark of Quarterdeck Office Systems, Inc. SyncComplete and TrendComplete are Trademarks of Kamsman Corporation. UnixWare is a registered trademark of the Santa Cruz Operation, Inc. UNIX is a registered trademark of X/Open Co., Ltd. XNS is a trademark of Xerox Corporation. NuBus is a trademark of Texas Instruments Incorporated.

Contents

1 Overview of ManageWise 2.6

ManageWise Features	1
ManageWise Components	2
ManageWise Concepts	6
ManageWise Agents	7
NetWare Management Agent	8
NetWare LANalyzer Agent	9
Introduction to the ManageWise Console	10
Starting the ManageWise Console	10
Exiting the ManageWise Console	10
ManageWise Console Window	11
Using Menu Commands	12
Displaying Information about Alarms	12
Items in the ManageWise Program List	12
ManageWise Icons on Your Startup Bar	13
ManageWise Maps	14
Exporting and Printing ManageWise Data	15
Setting Preferences in the ManageWise Console	15

2 Upgrading from ManageWise 2.5

Upgrade Issues Related to the ManageWise Console	17
Upgrade Issues Related to the ManageWise Server	18
Migrating Previously Installed Third-Party Software	18

3 Initial Setup for User Management

Task Overview	19
Adding Users to the MANAGEWISEGROUP User Group	19
Managing Other User Groups	20
Adding User Management Information to Login Scripts	20
Using Profile Objects to Manage Clients (NDS)	21

4 Initial Setup for Managed Computers

Task Overview	24
Functionality for Managed Computers	25
Setting Up Desktop Manager Support for NetWare Servers.	25
Copying files Needed to Manage a NetWare Server.	26
Modifications to the AUTOEXEC.NCF File.	26
ManageWise User Management NLM Files	27
USER.NLM	27
LDISCAN.NLM	27
Setting up User Management on Client Workstations and NT Servers	28
Configuring DOS Clients	28
Configuring Windows 3.x, Windows 95, Windows 98 Clients	29
Configuring VLM 1.2.1 Clients on Windows 3.x	31
Setting Options with Windows Client Configuration Program	31
Configuring Windows NT Clients.	32
Setting Options with Windows NT Configuration Program	33
Configuration of Windows NT machines which do not have Novell Client32 for Net- ware networks	34
Configuring OS/2 Client Workstation Software.	36
Configuring Macintosh Client Workstation Software	38

5 Setting Up the NetExplorer Discovery System

Introduction to NetExplorer Setup	39
Do You Need to Change the Default Configuration?.	39
Upgrading from ManageWise 2.5	40
NetExplorer Console Configuration Utility	40
Task Overview	41
Starting Discovery Initially	42
Step 1: Load the NetExplorer NLM Files	42
Step 2: Start NetExplorer Manager.	42
Checking the Status of Initial Discovery	43
Changing the NetExplorer Server Configuration.	45
Configuration Summary for the NetExplorer Server	45
Changing Which NetExplorer Modules Are Loaded	45
Changing SNMP Community Names	47
Changing the Discovery Scope	48
Hints to Ensure Complete Discovery	48
Changing the IP Discovery Scope	48
Changing the IPX Discovery Scope	50
Changing the Discovery Schedule	51
Loading and Unloading NetExplorer NLM Files	54
Changing NetExplorer Manager Settings	55
Configuration Summary for NetExplorer Manager	55
Configuring the NetExplorer Manager Schedule	55

Starting NetExplorer Manager Manually	57
Closing NetExplorer Manager	57
6 Setting Up AntiVirus Protection	
Setting up InocuLAN for NetWare Server Software	59
InocuLAN for NetWare Domain Manager	60
Installing InocuLAN on a Windows NT Workstation.	60
Possible Setup Tasks for AntiVirus Protection	61
Create an InocuLAN for Macintosh Install Disk	61
Creating a Macintosh Install Diskette	62
7 Initial Setup in the ManageWise Console	
Setting Up ManageWise Security	64
Setting Up ManageWise Console Security	64
Setting the ManageWise Console Password	65
Logging In to the ManageWise Console.	65
Editing a Default Security Template for Chat or File Transfer.	65
DOS Security	66
Windows NT Security	66
Checking the Results of Discovery	68
Evaluating the NetExplorer Manager Schedule.	68
Setting Up Alarm Handling	69
Enabling Alarms.	69
Changing Default Alarm Dispositions	69
Changing Alarm Thresholds.	70
Additional Tasks to Enhance Network Management	71
Creating Baseline Documents.	71
Creating a Custom Map of Critical Nodes on the Network	71
Adding Additional Details to the ManageWise Database	72
8 Configuring ManageWise Agents	
Configuring NetWare Management Agent	73
Task Overview for NetWare Management Agent Configuration	74
Changing Security Settings for SET and GET Operations	74
Changing NLM File Load Parameters.	75
Changing Trend Values in NTREND.INI	75
Changing Alarm Threshold Values in NTREND.INI	75
Controlling How Alarm Generation Occurs	76
Sending Alarms to non-ManageWise Management Stations	76
Limiting Transmission of SAP Packets from ManageWise Consoles	77
Configuring NetWare LANalyzer Agent	77
Task Overview for NetWare LANalyzer Agent Configuration	77
Improving the Performance of NetWare LANalyzer Agent	77

Enabling or Disabling Network Monitoring by Selected Network Adapters . . .	78
9 Installing Desktop Remote as a Standalone Application	
Introduction to Desktop Remote	79
Modem Requirements	80
Remote System Requirements.	80
Installing Desktop Remote as a Standalone Application.	80
10 Integrating Third-Party Applications	
Small-to-Medium Network Scenario	83
Medium-to-Large Network Scenario	84
What to Record about Third-Party Applications	86
Prerequisites to Installing Third-Party Software	86
Third-Party Installation Hints	87
Migrating Previously Installed Third-Party Software	88
A Troubleshooting Installation and Startup	
Troubleshooting the ManageWise Server	89
Problem: Server Halts (Abends)	89
Problem: Installation Cannot Copy .NCF Files	90
Problem: Short-Term Memory Allocation Failures	91
Decreasing Memory on the ManageWise Server	91
Decreasing the Maximum Packet Receive Buffers	91
Decreasing the Maximum Physical Receive Packet Size	91
Troubleshooting NetWare LANalyzer Agent Software	92
Receiving Token Ring Alarms	92
IPX, Network Boards, and Segment Monitoring	92
Changing Network Boards	93
Problem: Inaccurate NetWare LANalyzer Agent Statistics	93
Problem: Missing Bar Chart in the Network Dashboard Window.	93
Troubleshooting the ManageWise Console	94
Problem: Sluggish ManageWise Console	94
Problem: Internetwork Map Is Empty after ManageWise Runs for a While	95
Problem: Incomplete Internetwork Map after ManageWise Runs for a While	95
Troubleshooting Your Windows Environment	96
Troubleshooting Your Btrieve Environment	97
How You Need to Load BSTART.NCF	97
Problem: LDISCAN.EXE Runs Out of Memory.	97
Problem: Conflicts between Btrieve and Other Applications	97
Problems with the Inventory Manager Database	98
Problem: Records Not Listed in the Inventory Manager Database.	100
Troubleshooting Desktop Management Problems	100

Problem: You Get a Message about Loading SNMP VLM Files	100
Problem: Login Script Does Not Execute Properly	101
Problem: You Cannot Control the Keyboard on a File Server with Desktop Management 101	
Resolving Time Discrepancies	101
Troubleshooting Your WAN Environment	102
Technical Support and Update Information	102
How to Request Technical Support	102
How to Obtain Updates and Patch Files	102
Virus Protection	102
ManageWise	103
B Error Messages	
C ManageWise Server Backups	
Server Backups and NetWare LANalyzer Agent Files	113
Server Backups and NetExplorer Files	113
D Changes Install Makes to the ManageWise Server	
Server Installation Notes for Network Management.	116
Overview of Network Management Installation on the ManageWise Server .116	
Modifications to the AUTOEXEC.NCF File	116
Installation of the LANZ.NCF File	117
Installation of the NETXPLOE.NCF File.	117
Installation of the NMA2.NCF File	117
Installation of the NMA5.NCF File	117
Installation of the NMSBASE.NCF File	117
Server Installation Notes for Desktop Management	118
Overview of Desktop Management Installation on the ManageWise Server .118	
Modifications to the AUTOEXEC.NCF File	118
NetWare Login Script Changes to Support User Management	119
Support for Temporary Drive Mapping	120
Inventory Scan Programs	121
Loading and Configuring User Agents on DOS Workstations.	122
Bindery Objects Created by ManageWise	124
E Install Changes to the ManageWise Console and Workstations	
Changes to the SYSTEM.INI File	127
Changes to the WIN.INI File	127
F Changes Desktop Remote Makes to Your Workstation	

G NetExplorer Theory of Operations

NetExplorer System Components	131
NetExplorer Manager Software	133
NetExplorer NLM Software	134
Representation of Systems in the ManageWise Logical Maps	134
SAP IDs.	134
NetExplorer NLM Processes	135
NXPIP.NLM.	136
NXPIPX.NLM	137
NXPLANZ.NLM.	137
Additional ManageWise Components in a ManageWise Network	137
NetWare LANalyzer Agent Servers.	137
NetWare Management Agent Servers	138
NetWare Servers	138
NetExplorer Discovery Process	139
Continuous Discovery	139
Scheduled Discovery	140
NXPIP	140
NXPIPX.	141
NXPLANZ.	141
NETXPLO.	142
SNMP Community Name Discovery	142
NetExplorer Manager.	143
Names of Discovered Objects	145
Name Source Priority.	146
General Information about Naming.	146
Location Unknown Segment	147
What NetExplorer Discovers	147
Systems Discovered by NetExplorer	149
NetWare Servers	150
NetWare Client Workstations.	150
IP Routers	151
NetWare SFT III Servers	152
Systems Monitored by NetWare LANalyzer Agent	153
Systems Not Equipped with the IPX Diagnostic Responder	154
Routers That Use Duplicate MAC Addresses	154
Third-Party Routers.	156
NetWare MultiProtocol Router with WAN Ports	157
Third-Party Routers with WAN Ports	159
NetWare Connect Servers	159
Network Segments Discovered by NetExplorer	159
LAN and WAN Segment Types.	159
Source-Route Bridged Token Rings	160

Transparent Bridges.162

Configuration Changes162

Load Considerations for Running NetExplorer163

 28-Node Network Example164

 6530-Node Internetwork Example165

H Multiple ManageWise Servers in One NDS Container

Overview of ManageWise 2.6

The ManageWise® 2.6 product is a software platform consisting of a number of components for managing multivendor networks as a complete system. This chapter contains the following sections:

- ◆ “ManageWise Features”
- ◆ “ManageWise Components”
- ◆ “ManageWise Concepts”
- ◆ “ManageWise Agents”

ManageWise Features

ManageWise helps you manage your network by performing the following functions:

- ◆ Discovers your network devices and connections
- ◆ Monitors and manages servers, routers, and hub cards, and notifies you of potential problems on your network using real-time alarms
- ◆ Enables you to analyze your networks from a single management station
- ◆ Supplies a graphical view of your network by means of network maps that enable you to manage, control, and view information about devices on your network
- ◆ Provides summary information about server status and network performance anywhere on your network
- ◆ Enables you to control and monitor the DOS, Windows*, OS/2, and Macintosh workstations that are attached to your NetWare® network from your desk

- ◆ Enables you to communicate directly with workstations on your network using a two-way, split-screen dialog box
- ◆ Enables you to access and control your network from a remote location
- ◆ Collects and stores hardware and software information about the nodes on your network
- ◆ Enables you to manage your network print queues
- ◆ Provides continuous and on-demand virus scanning on servers and workstations
- ◆ Provides Inventory MacScan, which enables you to use Inventory Manager to collect and store hardware and software information about Macintosh* platforms connected to a ManageWise Server
- ◆ Provides remote access, chat, file transfer, and hardware and software inventory of DOS, Windows* 3.x, Windows 95*, Windows 98*, and Windows NT* workstations.

ManageWise Components

ManageWise is composed of the following components:

- ◆ ManageWise Console software

The ManageWise Console runs on a Windows 95, Windows 98 or Windows NT 4.x workstation. It provides services for managing networking resources, Interwar servers, hubs, and routers in a graphical interface. You can also manage your workstations from the ManageWise Console, for example, controlling workstations remotely, monitoring print queues.

- ◆ ManageWise Server software

Refer to Table 1-1 for a description of various Console, Server and client workstation components.

Table 1-1
ManageWise Components

Component	Function	Where Installed
ManageWise Console software components:	Provides user interface, Alarm Manager, Database Administration Tool, Segment Consolidation Tool, and online Help system.	Windows 95, Windows 98, Windows NT 4.x workstation.
Alarm Monitor	Receives and displays real-time alarms from the Alarm Manager that are forwarded with the appropriate alarm disposition.	Windows 95, Windows 98, Windows NT 4.x workstation.
SNMP Data Server	Manages devices using SNMP over IP and IPX™ protocols.	Windows 95, Windows 98, Windows NT 4.x workstation.
NetExplorer™ Manager	Sends requests to NETXPLOER.NLM on the ManageWise Server to retrieve the discovered information. Obtains discovered network data and topology devices, and stores this information in the ManageWise database.	Windows 95, Windows 98, Windows NT 4.x workstation.
Segment Consolidation Tool	Enables you to manually combine multiple segments in ManageWise maps into a single segment.	Windows 95, Windows 98, Windows NT 4.x workstation.
Database Administration Tool	Enables you to back up, reset, and purge alarms and restore your database.	Windows 95, Windows 98, Windows NT 4.x workstation.
ManageWise Client Workstation software components:		
CLNTCFG.EXE	Prepares each workstation for access by Desktop Manager.	Windows 3.x, Windows 95, Windows 98 workstations.
WUSER.EXE	Enables Desktop Manager to take control of and obtain diagnostic information from client workstations.	Windows 3.x, Windows 95, Windows 98 workstations.
WUSER32.EXE	The service loaded on the target workstation that enables the different features of Desktop Manager.	Windows NT workstations

Table 1-1 *continued*

ManageWise Components

Component	Function	Where Installed
NTSTACFG.EXE	A configuration program that installs the User Agents on the target workstations.	Windows NT workstations
OS2SETUPEXE	A configuration program that loads the User agents on the target workstations.	OS/2 workstations
USEROS2.EXE	The service loaded on the target workstation that enables the different features of Desktop Manager.	OS/2 workstations
DOSCFG.EXE	A configuration program that installs DOS User agents on the target workstations.	DOS workstations
USERTSR.EXE	A TSR loaded on the target workstation that enables the real-time features of Desktop Manager	DOS workstations
POPUPTSR.EXE	A TSR required for Chat, File Transfer, Run Program, and permission required features.	DOS workstations
LDAPPL.INI	A file that records software description. This file is used by the scan program to identify the software on workstations.	Server/workstations
LDISCAN.EXE	A program that scans workstations for inventory information.	DOS workstations
WLDISCAN.EXE	An inventory scanner for the target workstations.	Windows 3.x , Windows 95, Windows 98 workstations
LDISCNNT.EXE	An inventory scanner for the target workstations.	Windows NT workstations
LDISCAN2.EXE	An inventory scanner for the target workstations.	OS/2 workstations
Inventory MacScan	An inventory scanner for the target workstations.	Macintosh workstations
LDISCAN.CFG	A configuration file which stores the DeviceIDs that the Inventory Server assigns to each workstations.	All scanned workstations
TYPES.DAT, VALUES.DAT, MACHINES.DAT, FILES.DAT	Data files that make up the inventory database.	Servers

Table 1-1 *continued***ManageWise Components**

Component	Function	Where Installed
ManageWise Server software components:	Provides updated server data to the ManageWise Console.	NetWare 4.1x or NetWare 5 server.
NXPCON.NLM	Provides interface for configuring and monitoring the NetExplorer discovery system on your ManageWise Server.	NetWare 4.1x or NetWare 5 server.
NETXPLO.R.NLM	Communicates with other NetExplorer components to collect network discovery data. Downloads discovered data to your ManageWise Console when requested.	NetWare 4.1x or NetWare 5 server.
NXPIPX.NLM	Discovers IPX network devices, segments to which they are connected, and other information, such as services on systems.	NetWare 4.1x or NetWare 5 server.
NXPIP.NLM	Discovers IP routers, segments to which they are connected, and IP addresses.	NetWare 4.1x or NetWare 5 server.
NXPLANZ.NLM	Discovers all devices on segments where NetWare LANalyzer® Agent™ software is installed.	NetWare 4.1x or NetWare 5 server.
SERVINST.NLM	Implements the NetWare Server Management Information Base (MIB).	On every ManageWise Server.
NTREND.NLM	Implements the Threshold and Trend MIB.	On every ManageWise Server.
NWTRAP.NLM	Generates alarms when user-configured parameters are exceeded.	On every ManageWise Server.
HOSTMIB.NLM	Implements the standard Host Resources MIB [RFC 1514] and Novell's extensions to the Host Resources MIB.	On every ManageWise Server.
FINDNMS.NLM	Discovers workstations running the ManageWise Console.	On every ManageWise Server.
NDSTRAP.NLM	Implements the NetWare Directory Services (NDS®)Trap Management Information Base (MIB).	On every ManageWise Server (NetWare 5 Only).

Table 1-1 *continued*

ManageWise Components

Component	Function	Where Installed
LDINV.NLM	Coordinates access to and maintenance of the inventory database and supplemental log files.	On the ManageWise Server running Inventory Manager.
SCAN.INI	Keeps distributed LDAPPL.INI files current with the LDAPPL.INI file in the core server's network directory.	Servers
USER.NLM	Enables Desktop Manager to take control of and obtain diagnostic information.	On any server.
LDISCAN.NLM	Scans file servers to discover all hardware and software installed on the server.	On any server.

ManageWise Concepts

You need to know the following terms and concepts when setting up and using ManageWise:

Agent	Software component installed on a server that prepares, accumulates, and remotely communicates information to the management software component.
Discovery	Process of identifying network devices, determining the internetwork topology, and storing this information in the ManageWise database, which is part of the ManageWise Console. The ManageWise Console then uses the database to create maps. In ManageWise, discovery is done by NetExplorer on the ManageWise Server.
Discovered objects	Internetwork topology objects, such as servers, routers, hubs, segments, and IP and IPX networks that NetExplorer has identified.
NetExplorer	Term often used to refer to all the network discovery components that reside on the ManageWise Server, such as NETXPLO.NLM, and the ManageWise Console, such as NetExplorer Manager.
NetExplorer Manager	Component of the NetExplorer discovery system that resides on the ManageWise Console. NetExplorer Manager controls the timing and duration of updates from NetExplorer components on the ManageWise Server. NetExplorer Manager also keeps track of the records that were sent previously and directs NETXPLO.NLM to start with a specified record number. This enables multiple ManageWise Consoles to receive data from the ManageWise Server, as needed.

NetExplorer discovery system	Complete ManageWise network discovery software that has components on the ManageWise Server (NETXPLOE.NLM, NXPIP.NLM, NXPLANZ.NLM) and on the ManageWise Console (NetExplorer Manager). The ManageWise Server components discover segments, networks, and devices, and provide data to NETXPLOE.NLM. At the request of NetExplorer Manager, NETXPLOE.NLM sends data about new or changed objects to NetExplorer Manager.
NetExplorer Server	The ManageWise Server on which the NetExplorer NLM™ files and the NetExplorer configuration utility (NXPCON) are installed.
ManageWise Console	The workstation running Windows 95, Windows 98 or Windows NT on which you installed ManageWise. The ManageWise Console software includes the ManageWise graphical user interface, database, alarm system, and NetExplorer Manager. It also includes Desktop Manager Tools and virus protection software. The console communicates with agents on the LAN using SNMP. It collects data about the network devices. Use the console to display, review, manage, or acknowledge the data.
ManageWise Server	NetWare 4.1x or NetWare 5, NetWare SFT III™, NetWare/IP™, or SMP server on which ManageWise is installed. The ManageWise Server software consists of NetWare Management Agent™ software and can include NetExplorer, NetWare LANalyzer Agent, Desktop Management and Inventory Manager software, and the virus protection software.
InocuLAN Server	ManageWise Server on which the Cheyenne InocuLAN* virus protection software is installed.
Third-party applications	Plug-in software purchased separately that enhances the ManageWise platform.
Client	A node or workstation on a network that requires services from a server.
Segment	A component of a networking environment that corresponds to a physical cable. A segment is terminated by a bridge, a router, or any connecting device other than a repeater or hub. (ManageWise does not discover bridges, so sometimes ManageWise displays multiple bridged segments as a single segment.)

ManageWise Agents

ManageWise installs agents to enhance ManageWise functionality. You can use any or all of the agents, install them in any order, and deploy them at strategic locations in your network to perform four main functions:

- ◆ Gather useful information from servers and clients and make it available to the ManageWise Console

- ◆ Alert you through alarms to the ManageWise Console when problem conditions occur on your network
- ◆ Carry out commands issued by the ManageWise Console
- ◆ Log performance and trend information

Table 1-2 lists ManageWise agents.

Table 1-2
ManageWise Agents

Component	Where Installed
NetWare Management Agent (required)	Every NetWare 3.1x, NetWare 4.1x or NetWare 5, NetWare for OS/2*, SMP, NetWare/IP, and SFT III server that you want to manage.
NetWare LANalyzer Agent	One server (NetWare 4.x; NetWare 5, SMP; NetWare/IP; and SFT III) on each segment you want to monitor.

NetWare Management Agent

NetWare Management Agent software provides dynamic server performance data and information about server alarms to the ManageWise Console. This is a required component of ManageWise and is part of the ManageWise Server installation.

ManageWise can manage any NetWare server that has NetWare Management Agent software installed. The NetWare Management Agent software responds to management data requests from the ManageWise Console and also transmits alarms from the server to the ManageWise Console.

For each managed server, you can obtain the following real-time information:

- ◆ Configuration data
- ◆ Server utilization
- ◆ NetWare Loadable Module™ (NLM) files that are running
- ◆ Disk and volume usage

- ◆ Trends of key server statistics
- ◆ Memory usage
- ◆ Print status
- ◆ Bind information
- ◆ Interface data
- ◆ Connections
- ◆ Users logged in

You can also set and monitor alarm thresholds for critical server parameters.

NetWare LANalyzer Agent

NetWare LANalyzer Agent enhances the discovery process by enabling NetExplorer to monitor all traffic on network segments to which the server is attached. You can use NetWare LANalyzer Agent to obtain information about non-IPX stations and IP addresses for stations that use TCP/IP. NetWare LANalyzer Agent can monitor Ethernet, token ring, and FDDI segments. A single NetWare server, used as a router and running NetWare LANalyzer Agent, can monitor several network segments simultaneously.

NetWare LANalyzer Agent provides the following information and functions:

- ◆ General performance statistics and trends for all traffic on the segment.
- ◆ Viewing historical as well as current trends for all traffic on the segment.
- ◆ Detailed statistics for each station on the segment, including current information about the stations that are the busiest network users and conversation statistics that show how each station on the network communicates with other stations on the network.
- ◆ Detection of network overload, excessive errors, and stations with duplicate IP addresses.

- ◆ Monitoring of inactive nodes on a segment.
- ◆ Error reports sent immediately to the ManageWise Console.
- ◆ Packet capture, enabling you to specify the filtering criteria for packet capture. You can decode and view the captured packets at the ManageWise Console to help you analyze your network operations and identify the source of network problems.

Introduction to the ManageWise Console

The ManageWise Console includes the ManageWise graphical user interface, the alarm and topology database (referred to as the ManageWise database), an alarm system, and NetExplorer Manager. It also includes desktop management tools and anti-virus software.

Starting the ManageWise Console

To start the ManageWise Console

Procedure



1. Start Windows.

If you selected to run NetExplorer Manager continually (default), NetExplorer Manager appears on your desktop each time you start Windows.

Note



NetExplorer Manager runs in the background. NetExplorer Manager is active when the NetExplorer Manager icon appears in the Windows Task Bar.

2. Select ManageWise Console from the Program list.

The Alarm Manager and SNMP Data Server components are launched, the icons appear in the Windows Task Bar, and the ManageWise Console window is displayed. See Figure 1-1 for an illustration of the ManageWise Console window.

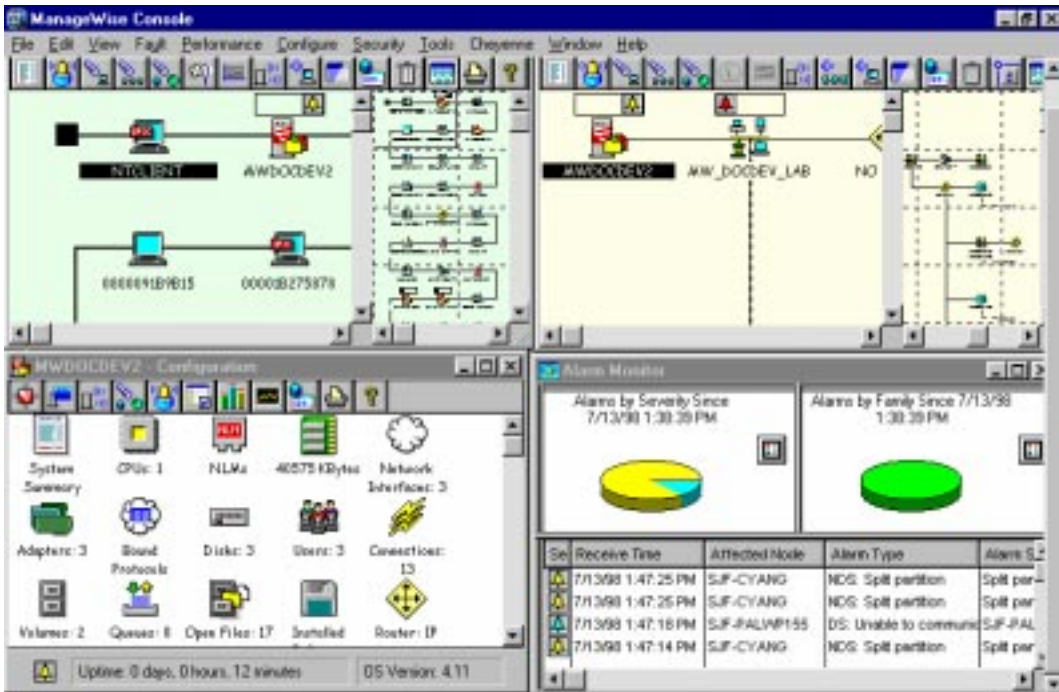
Exiting the ManageWise Console

To exit the ManageWise Console, select *File > Exit* or exit by using any standard Windows procedure.

Select the Close All Open ManageWise Components Upon Exit check box if you want ManageWise components closed automatically for you every time you exit ManageWise—the Alarm Manager, SNMP Data Server, and NetExplorer Manager (if it is running) icons disappear from from the Windows Task Bar.

ManageWise Console Window

Figure 1-1
ManageWise Console Window



The status bar spans the bottom of the ManageWise Console window. It includes the following fields:

Alarm icon—Indicates that an alarm is received.

Ticker tape—Describes alarms configured to be displayed in the ticker tape when an alarm is received.

Progress icon—Indicates progress of a long operation, such as opening and displaying a large internetwork map.

Date—Displays the current date.

Time—Displays the current time.

Using Menu Commands

You start ManageWise procedures by selecting menu commands or by selecting objects on maps and other displays. Some operations require you to select an object before you select a menu command.

Displaying Information about Alarms

You can access information about alarms in these places:

- ◆ Alarm Monitor, which displays all alarms as they are received. (Select *Fault > Alarm Monitor*.)
- ◆ Alarm Report, which displays alarms that are logged to the ManageWise database. (Select *Fault > Alarm Report*.)

Refer to the *ManageWise 2.6 Network Management Guide* or the ManageWise online Help for more information about alarm severity, displaying alarm information, and acknowledging alarms.

Items in the ManageWise Program List

The following items appear in the ManageWise Program list:

- ◆ ManageWise Console: Starts the ManageWise Console software.
- ◆ ManageWise README File: Provides late-breaking information about ManageWise.
- ◆ Post-Installation Setup Help: Provides steps that you might need to perform after installing ManageWise software. Be sure to review this Help file.
- ◆ ManageWise Setup Summary: Provides an installation log, which is useful for troubleshooting any installation problems.

- ◆ NetExplorer Manager: Obtains discovery information from the NetExplorer Server to update the ManageWise Console database.
- ◆ Segment Consolidation Tool: Starts the Segment Consolidation Tool, which you use to combine segments on maps.
- ◆ Database Administration Tool: Starts the Database Administration Tool, which you use to back up, reset, and restore your database.

ManageWise Icons on Your Startup Bar

Icons appear on the Windows Task Bar when each of the following components is running.

- ◆ NetExplorer Manager: An icon appears on your desktop when NetExplorer Manager is running. You can shut down this component by clicking the right mouse button when the mouse cursor is over the button in the Windows Task Bar, click Close from the context menu.
- ◆ SNMP Data Server: This component is a background process that starts when you start the ManageWise Console. The SNMP Data Server is responsible for communicating with SNMP-manageable nodes on the network (receiving incoming data, such as alarms, and sending data to the nodes.) You can shut down this component by clicking the right mouse button when the mouse cursor is over the button in the Windows Task Bar, click Close from the context menu.
- ◆ Alarm Manager: This component is a background process that starts when you start the ManageWise Console. The Alarm Manager receives alarms from data acquisition modules, applies appropriate disposition to the alarms, and displays them in the ManageWise Console. You can shut down this component by clicking the right mouse button when the mouse cursor is over the button in the Windows Task Bar, click Close from the context menu.

These components can continue to run after you exit the ManageWise Console if you do *not* close all ManageWise components when you exit the ManageWise Console.

ManageWise Maps

When NetExplorer discovers your network, it gathers information about objects on your network and places them in the ManageWise database. ManageWise maps use this data to show your network's topology.

There are three types of ManageWise maps:

- ◆ The *internetwork map* provides an overview of the logical organization of your network. It shows all IPX routers (and IP routers if your network runs TCP/IP), Ethernet segments, token ring segments, FDDI, and other network types.

To view an internetwork map, select *File > Open > Internetwork Map* from the ManageWise Console window.

- ◆ The *segment maps* are maps that ManageWise builds for each segment shown on the internetwork map. They display servers, workstations, routers, and other devices attached to the segment.

To view a segment map, perform *one* of the following actions:

- ◆ Double-click the icon on a desired segment in an open internetwork map.
- ◆ Select the segment icon in an open internetwork map and select *File > Open > Segment Map*.
- ◆ Select *File > Open > Segment Map*, and then select the segment by segment ID or name.
- ◆ The *custom map* enables you to create a custom view of your network. You can, for example, represent the location of networks, segments, and devices relative to your geographic location. Alternatively, you can create a map that shows only the servers and routers you monitor daily. Custom maps also enable you to specify the connection between logical and physical networks.

To create a custom map, you must understand and use the Custom Map Editor window, which you access by selecting *Edit > Custom Map > New*. The Custom Map Editor window contains action bar buttons that enable you to perform distinct functions within the Custom Map Editor.

For information about adjusting your maps after initial discovery and creating and using custom maps, refer to the discovery chapters in *ManageWise 2.6 Network Management Guide*.

Exporting and Printing ManageWise Data

You can print and export many types of ManageWise data. Look for icons in the various windows and dialog boxes to help you do so or use the Print and Export menu commands. TrendComplete™ and SyncComplete™, two other features that help you gather and analyze data, include reporting functions.

You can use ManageWise data for reports, troubleshooting, or inventory control. For example, you can use ManageWise network data in these ways:

- ◆ Print the network inventory. Print a map of the segments and routers on your network and then print maps of the servers, routers, workstations, and other devices on each segment. Use the collected maps as a basic network inventory.
- ◆ Print and assemble a collection of maps of a particular segment to show the workstations that are connected to a segment.

To obtain information about segment use and network growth you can print maps when you first use ManageWise, which creates a background. You can then print maps at regular intervals and compare those maps against your baseline. For a true comparison, however, you must reset your ManageWise database and rerun NetExplorer. This is because information about any nodes that were removed from the network are still in the database.

You can also extract information from the database by using query systems with report writers, such as SQLSCOPE from BTI or Crystal Reports.

Setting Preferences in the ManageWise Console

By selecting the *Configure > Global Preferences* command, you can change global preferences for options such as

- ◆ Path to the ManageWise database directory. This path is set during installation. The path can be changed, for example, if you need to

move the database because the hard disk of the ManageWise Console becomes full.

- ◆ Server that is running the NetExplorer NLM software (the ManageWise Server). During installation, the NetExplorer Server is identified.
- ◆ Background color for maps.

2 *Upgrading from ManageWise 2.5*

This chapter describes your tasks and the tasks ManageWise® software does for you when upgrading from ManageWise 2.5 to ManageWise 2.6. You can upgrade only from ManageWise 2.5, not from earlier versions of ManageWise.

This chapter contains the following sections:

- ◆ “Upgrade Issues Related to the ManageWise Console”
- ◆ “Upgrade Issues Related to the ManageWise Server”
- ◆ “Migrating Previously Installed Third-Party Software”

Upgrade Issues Related to the ManageWise Console

Component/Settings	Action
ManageWise database	Select the option in the installation program to indicate whether you want to preserve your existing ManageWise database (alarm and topology database).
Global preference settings, for example, background color of maps	Setup saves the NMS.INI file to NMS.SAV. If you want to keep the global settings, copy the settings related to global preferences from NMS.SAV to NMS.INI or set them again through the ManageWise user interface.

Upgrade Issues Related to the ManageWise Server

Component/Settings	Action
NetExplorer settings	If you upgrade from ManageWise 2.5, the NetExplorer™ software saves configuration information from the NXP.INI file to SYS:\NMDISK\BACKUP\xxx. Refer to this backed up information when you reconfigure NetExplorer using the NXPCON utility.

Migrating Previously Installed Third-Party Software

If you are upgrading ManageWise and have third-party applications installed, you might need to compare the backup copy of your NMS.INI file to the new NMS.INI file to see whether any entries affecting previously installed software were changed.

chapter **3** *Initial Setup for User Management*

ManageWise® installation prepares the ManageWise server so that NetWare clients logging in to a ManageWise server can be centrally managed from the ManageWise Console. You will need to perform some server configuration to manage all of the users that you want to in your organization.

Task Overview

Table 3-1
Setup Overview for User Management

Task	Setup Required?	Refer to
Add users to the MANAGEWISEGROUP user group	Required	"Adding Users to the MANAGEWISEGROUP User Group" on page 19.
Manage groups other than the MANAGEWISEGROUP user group	Optional	"Managing Other User Groups" on page 20.
Manage users who are not in the same OU as the MANAGEWISEGROUP user group	Optional	"Adding User Management Information to Login Scripts" on page 20. or "Using Profile Objects to Manage Clients (NDS)" on page 21.

Adding Users to the MANAGEWISEGROUP User Group

When you install the ManageWise software, the installation program creates a MANAGEWISEGROUP user group in the container that the ManageWise server exists in. The ManageWise installation places the administrator-equivalent account, that you used during installation, directly into the MANAGEWISEGROUP user group. You have to add the other users that you want managed to MANAGEWISEGROUP user group manually, using the

NetWare Administrator utilities. All users added to the MANAGEWISEGROUP user group will be automatically setup with ManageWise user management agents at login.

Managing Other User Groups

After installation, you might want to create another group of users that will also be managed. The ManageWise installation grants certain rights to the MANAGEWISEGROUP user group. If you want another group to be managed, you must grant the appropriate rights manually. Any user you want managed must have the following rights to the specified directories on the ManageWise Server:

SYS:\MW\LDT	RF
SYS:\MW\LDT\SELTEMP	CRWEMF
SYS:\MW\INOCULAN	RF
SYS:\MW\INOCULAN\TEMP	CRWEMF

where C=Create, R=Read, W=Write, E=Erase, M=Modify, and F=FileScan.

Use the NetWare Administrator utilities to grant the appropriate rights to the group.

Adding User Management Information to Login Scripts

On NetWare® 4.x and NetWare 5 servers using bindery emulation and on NetWare 3.x servers, the ManageWise installation program modifies the System login script and the NDS* container login script. By default, the ManageWise Setup modifies the login script to perform setup and loading of the ManageWise client utilities.

If the users that you want to manage are not in the same OU container as the MANAGEWISEGROUP user group, you must substitute the full path to the MANAGEWISEGROUP user group.

For example

```
IF MEMBER OF ".Managewisegroup.MyOU.MyCompany" THEN
```

For more information about creating and using login scripts, see the NetWare documentation for your network operating system.

Using Profile Objects to Manage Clients (NDS)

An alternative to using the container login script to add ManageWise commands is to create a Profile login script that contains the ManageWise commands. Then, for each user that you want to manage, you can specify that the user run the Profile login script.

To manage clients using a profile login script, follow these steps:

Procedure



1. **Run NetWare Administrator (NWADMIN) from Windows.**
2. **Create a Profile object by selecting *Object > Create* and then selecting *Profile* from the list of object types.**
3. **Give the Profile object a name, select the Define Additional Properties check box, and then select *Create*.**
4. **Select the Login Script page from the resulting window, and then enter the ManageWise commands or copy the following text and paste it into login script, after the mapped search drives but before the first EXIT statement. Replace the <variable> indicators with the appropriate text for your server and context (remove the < and > when you do so).**

```
REM *** BEGIN ManageWise Desktop Management Section ***
IF MEMBER OF ".MANAGEWISEGROUP.<context>" THEN
MAP ERRORS OFF
MAP ins S1:=L:
MAP L:=<ManageWiseServerName>\SYS:
INCLUDE L:\PUBLIC\MW_LOGIN.DAT
MAP L:=S1:
MAP del S1:
MAP ERRORS ON
END
REM *** END ManageWise Desktop Management Section ***
REM **** BEGIN ManageWise INOCULAN Virus Protect Section
IF MEMBER OF ".MANAGEWISEGROUP.<context>" THEN
```



```

IF <OS> = "WINDOWS_NT" THEN
REM  **NT WORKSTATION ** NOTHING TO DO
ELSE
MAP L:=<ManageWiseServerName>/SYS:
#L:\INOCULAN\AVUPDATE.EXE /Q
END
END
REM **** END ManageWise INOCULAN Virus Protect Section

```

5. **Bring up the Details window for the user, select the Login Script page, and, from the Profile box, select the ManageWise Profile object. (You need to do this for each user you want to manage.)**
6. **If you use Profiles to configure the users you want to manage, place “REM” at the start of the two IF MEMBER OF lines in the Profile login script. Also place “REM” at the start of the two lines containing the END statement.**
7. **You must grant each user rights to the Profile.**

To assign rights, otherwise known as trustee assignments, drag the user icon onto the Profile object, then click OK when the Trustee dialog box appears.

After configuring the ManageWise server and adding users to the MANAGEWISEGROUP user group. You can modify parameters for the client utilities. Continue on to the next chapter for information on configuring the ManageWise client utilities.

4 *Initial Setup for Managed Computers*

ManageWise® provides a central point of administration for managing server and workstation computers on NetWare networks. Managed computers can include:

- ◆ NetWare 3.1x, NetWare 4.1x, NetWare 5 servers
- ◆ Windows NT Server 3.5x and 4.0
- ◆ Windows NT Workstation 3.5x and 4.0
- ◆ Windows 98, Windows 95, Windows 3.1x, Windows for Workgroups 3.1x and MS-DOS 5.x or later workstations
- ◆ OS/2 2.1 or later workstations
- ◆ Macintosh workstations

This chapter provides information about tasks that you might want to do to get ManageWise user management programs up and running initially. You can refer to the *ManageWise 2.6 Desktop Management Guide* later for further customizing desktop management.

Task Overview

Table 4-1
Setup Overview for User Management

Task	Setup Required?	Refer to
Setting up a NetWare server to be managed	Optional	"Setting Up Desktop Manager Support for NetWare Servers" on page 25.
Setting up a NT server or NT workstation to be managed	Optional	"Setting up User Management on Client Workstations and NT Servers" on page 28.
Setting Up a Windows 98, Windows 95, Windows for Workgroups 3.1x, Windows 3.x, or DOS workstation to be managed	Optional	"Configuring DOS Clients" on page 28, and "Configuring Windows 3.x, Windows 95, Windows 98 Clients" on page 29.
Setting Up a OS/2 workstation to be managed	Optional	"Configuring OS/2 Client Workstation Software" on page 36.
Setting Up a Macintosh workstation to be managed	Optional	"Configuring Macintosh Client Workstation Software" on page 38.

ManageWise Desktop Manager must be installed on the ManageWise Console and server. Installation of Desktop Manager is performed by the ManageWise Installation program. If you selected not to install Desktop Manager during installation of ManageWise, run the ManageWise Installation again, choose the custom installation and select the option to install Desktop Manager.

After ManageWise Desktop Manager is installed, you will need to add all users to the MANAGEWISEGROUP user group that you want to manage from the ManageWise Console. You can refer to Chapter 3, "Initial Setup for User Management," for information on how to add users to the MANAGEWISEGROUP.

Functionality for Managed Computers

Managed computers can be controlled from the ManageWise Console. Table 4.1 lists ManageWise features supported for each type of managed computer.

Table 4-2

List of User Management Features and Supported Protocols

	IPX	Winsock TCP/IP
Windows 98, Windows 95, Windows for Workgroups, Windows 3.1x	Remote Control Chat File Transfer Reboot Inventory	Remote Control Chat File Transfer Reboot Inventory
Windows NT Workstation and Windows NT Server	Remote Control Chat File Transfer Reboot Inventory	Remote Control Chat File Transfer Reboot Inventory
NetWare Server	Remote Control Inventory	
DOS	Remote Control Reboot Inventory	
OS/2	Remote Control Inventory	
Macintosh	Inventory (IPX/AppleTalk)	

Setting Up Desktop Manager Support for NetWare Servers

ManageWise, by default, installs all files needed to manage the NetWare server to the SYS:\SYSTEM folder on the ManageWise server. If you want to control other servers from the ManageWise console you will need to copy the same files to the NetWare server and make modifications to the AUTOEXEC.NCF file.

Copying files Needed to Manage a NetWare Server

To install NetWare user management software to a NetWare server, do the following:

Procedure



1. Locate USER.NLM, and LDISCAN.NLM.

You can find the NLM files on the ManageWise server's SYS: volume in the SYSTEM folder.

2. Copy the files to the NetWare server that you want to manage.

Copy files to the NetWare server's SYS://SYSTEM folder.

3. Modify the AUTOEXEC.NCF file on the NetWare server that you want to manage, to load the NLM files (USER.NLM and LDISCAN.NLM) that you copied to the SYS://SYSTEM folder.

You can create a NCF file to load the NLM files that is called from the AUTOEXEC.NCF file.

Modifications to the AUTOEXEC.NCF File

The ManageWise installation places a command in the ManageWise server's AUTOEXEC.NCF file that calls the MW_AUTO.NCF file. This file consists of commands to load NLM files required by ManageWise to manage the server from ManageWise Console's Desktop Manager utility. If you manually install the management NLM files, described above, to a NetWare server you can model the method used by the ManageWise server.

The following lines are added to the ManageWise server's AUTOEXEC.NCF file:

```
REM *** BEGIN Desktop Management Section ***
      MW_AUTO.NCF
REM *** END Desktop Management Section ***
```

The ManageWise installation makes a backup of your current AUTOEXEC.NCF file before making these changes. The backup is named AUTOEXEC.00x.

The MW_AUTO.NCF file might consist of the following:

```
REM The following commands load the NLMs
REM by Desktop Manager.
LOAD USER
LOAD LDISCAN INV_SERV=<SERVERNAME> FILE=<SYS:MW\LDT>
SCANNOW
```

ManageWise User Management NLM Files

Each of the following NLM files can be loaded manually or from an .NCF file.

USER.NLM

USER.NLM enables you to remotely control a server with Desktop Manager. For more information about USER.NLM, refer to the *ManageWise 2.6 Desktop Management Guide*.

To load USER.NLM, type the following at the ManageWise Console:

```
LOAD USER
```

LDISCAN.NLM

LDISCAN.NLM is the server inventory scan NLM file. This NLM file scans the hardware and software on the server. You must specify an inventory server in the command line. The ManageWise server loads the LDINV.NLM to handle inventory requests from servers and workstations. A server running the LDINV.NLM can collect inventory information for a network. You should have only one inventory server on a network or network segment. To indicate the directory where the inventory initialization file is located, add a file= parameter to the command line. The default location on a ManageWise server is the <SYS:MW\LDT> directory. For more information about LDISCAN.NLM, refer to the *ManageWise 2.6 Desktop Management Guide*.

To load LDISCAN.NLM, type the following at the server console:

```
LOAD LDISCAN INV_SERV=<servername> FILE=<SYS:MW\LDT>
SCANNOW TIME=<#>
```

You can use TIME=# option to specify the time to run inventory scan. The TIME value can be set from 0 hours to 23 hours. Specify the

SCANNOW option to send the inventory of the server immediately. By default, the server is inventoried at 20:00 hours.

Setting up User Management on Client Workstations and NT Servers

User management requires that user agents be copied and configured on each workstation to be managed. Most of the process is handled by configuration programs that are launched when you login to the ManageWise server. Any member of the MANAGEWISEGROUP user group will have the client machine configured the first time they login to the ManageWise server or context that the ManageWise server is contained in. Windows NT servers and workstations require the user logging in to have administrator-equivalent permission on the NT machine. OS/2 workstations are not configured when logged into the ManageWise server, configuration for OS/2 workstations can be done manually as explained later in this chapter.

The user management agents enable ManageWise to gather real time statistics and to remote control computers connected to the network. Since not all users connected to the network are working on the same environment different user agents need to be configured for each environment. Users that are members of the MANAGEWISEGROUP user group will be configured with the appropriate user agent for their workstation's environment. But if you want to configure a workstation manually steps for doing so are provided in the following sections.

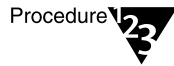
Configuring DOS Clients

ManageWise installs and configures DOS workstations with the user management software if the user belongs to the MANAGEWISEGROUP user group. When the user logs in to the ManageWise server as a member of MANAGEWISEGROUP the user agents are loaded from the include file MW_LOGIN.DAT. For information on how to add a user to the MANAGEWISEGROUP user group refer to, "Adding Users to the MANAGEWISEGROUP User Group" on page 19.

Note: InocuLAN and Desktop Manager workstation software can be installed and configured individually, but when installing workstation software together from the login script you will receive a message to reboot your workstation after the InocuLAN or Desktop Manager workstation software is installed. Ignore this

message until both the InocuLAN and the Desktop Manager software has been fully configured before rebooting your workstation.

To manually install a DOS user management agent, do the following:



1. Locate DOSCFG.EXE.

You can find DOSCFG.EXE on the ManageWise server's SYS:\\MW\\LDT\\ folder.

2. At the workstation, run DOSCFG.EXE.

This program copies the USERTSR.EXE, POPUPTS.R.EXE files and other required files for configuration to the MWCLIENT directory on the client machine. It also modifies the AUTOEXEC.BAT file to load the USERTSR and POPUPTS.R, at startup.

The DOS configuration program adds an entry for every DOS machine that has been configured into a file called CFG_YES.LOG. This log file is created on the inventory server under \\Inv_Server\\sys:mw\\ldt\\seltemp directory.

Before configuring a DOS machine, DOSCFG.EXE checks for an entry of that particular machine in the CFG_YES.LOG file and if there is one, it doesn't configure the DOS machine.

Note: The entry that is being added into the CFG_YES.LOG file is the DEVICEID generated during the scan and put into the LDISCAN.CFG file in the root directory of the DOS machine. In case this file is deleted or the DEVICEID is not found, then the DOSCFG.EXE will configure the machine a second time.

3. After DOSCFG.EXE is finished configuring your machine, exit the program and reboot the machine to load the user agent.

For more information about the user management agents, refer to the *ManageWise 2.6 Desktop Management Guide*.

Configuring Windows 3.x, Windows 95, Windows 98 Clients

ManageWise installs and configures Windows workstations with the user management software if the user belongs to the MANAGEWISEGROUP user group. When the user logs in to the ManageWise server as a member of MANAGEWISEGROUP the user agents are loaded from the include file MW_LOGIN.DAT. For

information on how to add a user to the MANAGEWISEGROUP user group refer to, “Adding Users to the MANAGEWISEGROUP User Group” on page 19.

Note: InocuLAN and Desktop Manager workstation software can be installed and configured individually, but when installing workstation software together from the login script you will receive a message to reboot your workstation after the InocuLAN or Desktop Manager workstation software is installed. Ignore this message until both the InocuLAN and the Desktop Manager software has been fully configured before rebooting your workstation.

To manually install a Windows user agent for management support, do the following:

Procedure



1. Locate CLNTCFG.EXE.

You can find CLNTCFG.EXE on the ManageWise server's SYS:\MW\LDT\ folder.

2. At the workstation, run CLNTCFG.EXE with the following command line:

```
CLNTCFG
```

CLNTCFG.EXE copies a file, WINCFG.TXT to the Boot drive under the Windows directory on the workstation. The Windows workstation will not be reconfigured, if WINCFG.TXT file is present on the workstation.

CLNTCFG.EXE uses a CLNTCFG.INI to setup the User agent (WUSER.EXE), and installs WUSER.EXE, WCHAT.EXE, WSLAVE.EXE and the required DLLS on the workstation to the \WINDOWS\SYSTEM directory of the Windows workstations.

It adds the following line in the WIN.INI file

```
LOAD=WUSER.EXE
```

On subsequent startup of Windows, WUSER.EXE is loaded.

Note:

- ◆ Delete the file, WINCFG.TXT to reconfigure the Windows workstation or use one of the CLNTCFG.EXE parameters discussed later in this section.

- ◆ The user on the Windows workstation has to login to the Inventory Server to execute CLNTCFG.EXE.
- ◆ CLNTCFG.EXE also adds a "LANDesk Client Configuration" section to the WIN.INI file that indicates that the workstation has been configured.
- ◆ When configuring Windows 3.x workstations, always use Novell IntraNetwork/NetWare Client for Windows 3.x login window to login as a user who is a member of the MANAGEWISE group.

Configuring VLM 1.2.1 Clients on Windows 3.x

You can configure VLM 1.2.1 on Windows 3.x by using the client configuration program CLNTCFG.EXE.

1. **From the DOS prompt, login to the inventory server as a member of MANAGEWISEGROUP user group and configure the workstation as a DOS client.**

Note



Do not reboot the workstation after configuring it as a DOS client. Start windows instead and continue with the steps to complete the client configuration process.

2. Desktop Remote is an ideal tool for the following situations:
 - Start Windows.
3. Run CLNTCFG.EXE from the SYS:\MWLDT\ directory of the ManageWise Server (inventory server).
4. Quit Windows and reboot the workstation.

Setting Options with Windows Client Configuration Program

The configuration program, CLNTCFG.EXE configures Windows 3.x, Windows for Workgroups, Windows 95, and Windows 98 workstations for Desktop Management.

CLNTCFG.EXE uses the following command-line syntax.

CLNTCFG.EXE [-M] [-F]

Table 4-3: CLNTCFG.EXE Command-line Parameters

Parameter	Description
-M	Specifies that the ManageWise User Agent (WUSER.EXE) and the related files will be installed overriding previous configuration of the ManageWise user management agent. If you want to over the Z.E.N.works Remote Control Agent use the -F parameter.
-F	Specifies that the ManageWise User Agent (WUSER.EXE) and the related files will be installed overriding the Z.E.N.works Remote Control Agent on Windows workstations. By default, the CLNTCFG.EXE detects the existence of Z.E.N.works Remote Control Agent on the workstation. If it exists, CLNTCFG.EXE does not install the ManageWise User Agent on the workstation.

Configuring Windows NT Clients

ManageWise installs and configures Windows NT workstations and servers with the user management software if the user belongs to the MANAGEWISEGROUP user group. When the user logs in to the ManageWise server as a member of MANAGEWISEGROUP the user agents are loaded from the include file MW_LOGIN.DAT. For information on how to add a user to the MANAGEWISEGROUP user group refer to, “Adding Users to the MANAGEWISEGROUP User Group” on page 19.

To manually install a Windows NT server or workstation with user management support, do the following:

Procedure



1. Locate NTSTACFG.EXE.

You can find NTSTACFG.EXE on the ManageWise server's SYS:\MW\LDT\ folder.

2. At the NT server or workstation, run NTSTACFG.EXE.

NTSTACFG.EXE uses a NTSTACFG.INI file, to setup the NT software. NTSTACFG.EXE program makes the following changes to the NT computer:

- ◆ Installs a remote control agent (WUSER32.EXE) to the workstation or NT server.
- ◆ Creates a ManageWise program folder with shortcuts.

For more information about the user management agents, refer to the *ManageWise 2.6 Desktop Management Guide*.

Setting Options with Windows NT Configuration Program

The configuration program, NTSTACFG.EXE configures Windows NT workstations for Desktop Management.

NTSTACFG.EXE uses the following command-line syntax.

NTSTACFG.EXE [/NOLOGON] [/NOREBOOT] [/IPX] [/IP/TCPIP]
[/NETBIOS] [/PROMPT] [/F] [/N/NOUI]

Table 4-4: NTSTACFG.EXE Command-line Parameters

Parameter	Description
NOLOGON	Specifies the workstation will not be configured using the login script.
NOREBOOT	Specifies the workstation will not be rebooted.
IPX	Specifies the protocol as IPX over which the ManageWise Console communicates with the workstation.
IP/TCPIP	Specifies the protocol as IP or TCPIP over which the ManageWise Console communicates with the workstation.
NETBIOS	Specifies the protocol as NETBIOS over which the ManageWise Console communicates with the workstation.
/F	Specifies that the ManageWise User Agent (WUSER32.EXE) and the related files will be installed overriding the Z.E.N.works Remote Control Agent on Windows NT workstation. By default, the NTSTACFG.EXE detects the existence of Z.E.N.works Remote Control Agent on the workstation. If it exists, NTSTACFG.EXE does not install the ManageWise Windows Agent on the workstation.
PROMPT	Asks the user before installing the Desktop Manager components on the workstation. By default, the prompt setting is set to off.
N/NOUI	Disables the User Interface dialog during the configuration of the workstation. By default, the UI mode is set to on.

Configuration of Windows NT machines which do not have Novell Client32 for Netware networks

The prerequisites to configure Windows NT machines which do not have Novell Client32 for NetWare networks are.

- ◆ All the NT machines should have IP stack and Client for Microsoft network installed.
- ◆ An NT server. The NT client configuration files are stored on this NT server.

Preparing for configuration of NT machines

ManageWise Installation will copy the required files on to an Inventory server(Netware). The following steps explain how to copy these files from the Inventory server(Netware) on to a Windows NT server. It is recommended to use a primary domain Windows NT server. Using the primary domain Windows NT server will help the Administrator, to create a login script to automate the inventory scanning for all the users. Choose a machine which has access to both Netware server and a NT server. On the machine, follow these steps:

- 1. Map a drive to the Window NT server's directory, which has read/write access for all the users.**

Example: M

M is the drive that maps to a public directory on the NT server.

- 2. Create a directory called LDT on the drive mapped to Windows NT server.**

Example: M:\> MD LDT

- 3. Change directory to SYS:<MANAGEWISEDIRECTORY>\LDT on the inventory server.**

<MANAGEWISEDIRECTORY> (by default, this directory is mw) specifies the directory, where ManageWise has been installed.

Example: CD J:\MW\LDT

J: is the drive that maps to the SYS volume of the inventory server.

- 4. Run NTONLY.BAT <DESTPATH>**

<DESTPATH> is the full path to LDT directory on the drive mapped to the NT server. The batch file(NTONLY.BAT) will copy the required configuration files to the NT server. It also copies the other batch files(INVENT.BAT and LDTINST.BAT) on the NT server.

Example: NTONLY M:\LDT

To configure Windows NT machines (which do not have Novell Client32 for NetWare networks)

- 1. Change directory to LDT directory on the NT server.**
- 2. Open INVENT.BAT file and modify according to the example shown in the file.**
- 3. Copy the modified INVENT.BAT to %SYSTEMROOT%\SYSTEM32\REPL\IMPORT\SCRIPTS directory on the NT Server.**

Include the batch file to the logon script for the required domain users, using User Manager utility provided in the Administrative tools. So that when the domain user logs in to this domain from any NT machine, an inventory scan of that NT machine will be done automatically.

- 4. Open LDTINST.BAT file and modify according to the example shown in the file.**

The batch file(LDTINST.BAT) should be run on all NT machines to configure them for remote control functionality. Ask all the users to map to the LDT directory on the NT sever and run the batch file(LDTINST.BAT). Configuring the NT machines for remote controlling should be done only once. The user should be an Administrator or Administrator-equivalent on the NT machine to configure the machine.

Configuring OS/2 Client Workstation Software

To manually install OS/2 client workstation software on an OS/2 workstation, do the following:

Procedure



- 1. Locate OS2SETUP.EXE.**

You can find OS2SETUP.EXE on the ManageWise CD-ROM (in the LDT\OS2 directory) or on the ManageWise server's SYS:\\MW\LDT\ folder.

- 2. At the OS/2 workstation, type OS2SETUP.EXE.**

OS2SETUP.EXE uses a configuration file, OS2SETUP.CFG, to install OS/2 client workstation software. OS2SETUP.EXE makes the following changes to the OS/2 workstation:

- ◆ Creates the LDISCAN and LDUSER directories and adds the appropriate files
- ◆ Adds DEVICE=<boot_drive>\LDUSER\VUSEROS2.SYS to the OS/2 workstation's CONFIG.SYS file
- ◆ Creates a MANAGEWISE LDUSER folder with a USEROS2 icon and a MANAGEWISE LDISCAN folder with a LDISCAN2 icon

3. Copy USEROS2.EXE from the MANAGEWISE LDUSER folder to the STARTUP folder.

Ensure that you copy USEROS2.EXE to the STARTUP folder and not the STARTUP.CMD batch file.

4. Add the following parameter to the LDISCAN2 properties dialog box:

```
/s=<inventoryservername>;
```

Replace the <variable> indicators with the appropriate text for your inventory server (remove the < and > when you do so).

5. Restart your OS/2 workstation.

Install OS/2 client workstation software on every OS/2 workstation that you want to manage.

OS2SETUP.EXE writes a command line to load an OS/2 version of the user agent. The user agent, USEROS2.EXE, is used to remotely control OS/2 workstations. Typically, USEROS2.EXE either runs under the Novell® NetWare Requester™ for OS/2 or utilizes Novell OS/2 32-bit networking Dynamic Link Libraries (DLLs). A third option is to run USEROS2.EXE under the IPX protocol.

For more information about the user management agents, refer to the *ManageWise 2.6 Desktop Management Guide*.

Configuring Macintosh Client Workstation Software

Inventory MacScan extends the reach of Inventory Manager to the Macintosh platform. It performs nearly all the functions of its DOS counterpart, LDISCAN.EXE, for Macintosh workstations connected to a ManageWise Server. For information on setting up virus protection on a Macintosh, refer to the InocuLAN AntiVirus Guide.

To install Inventory MacScan, follow these steps:

Procedure



1. Put the **MacScan** diskette into the disk drive.
2. Run the **MacScan Installer** program.

This program will install Inventory MacScan and the Readme file on Macintosh workstations. Inventory MacScan scans inventory on target Mac workstations. The Readme file provides information about the Inventory Scanner.

3. Choose the **Install** button.
4. Specify the destination folder to install Inventory MacScan.

Creates ManageWise Inventory MacScan folder.

5. Choose the **Save** button.

The Inventory MacScan program is installed on your hard disk. You can add the Inventory MacScan program to the system startup folder to launch the scanner at startup.

6. Open the **ManageWise Inventory MacScan** program.
7. To launch a scan select **File > Execute Scan**.

For more information about the user management agents, refer to the *ManageWise 2.6 Desktop Management Guide*.

Setting Up the NetExplorer Discovery System

NetExplorer™ software on a ManageWise® Server automatically discovers the nodes on your network. NetExplorer Manager on the ManageWise Console connects to the ManageWise Server and obtains the discovered data. ManageWise uses that data, which is stored in the ManageWise Console database, to create ManageWise maps.



Note Hereafter, the ManageWise Server on which NetExplorer software is installed is referred to as the NetExplorer Server. Typically, only one server on a network is a NetExplorer Server.

Introduction to NetExplorer Setup

This chapter includes information that helps you set up your NetExplorer system initially. Other options are available in the NetExplorer configuration utility, NXPCON, that are not discussed in this chapter. Refer to the *ManageWise 2.6 Network Management Guide* and to the NXPCON online Help (F1) for additional information.

For detailed information about the NetExplorer system, refer to Appendix G, “NetExplorer Theory of Operations.”

Do You Need to Change the Default Configuration?

The NetExplorer system is installed with configuration defaults designed to work in most environments. You do not have to make changes to NetExplorer to run ManageWise. However, if NetExplorer is discovering more than you want to be in your ManageWise database or if your network is not fully discovered, you need to reconfigure NetExplorer.

Review the following sections to determine whether you need to change any of the default configurations:

- ◆ “Configuration Summary for the NetExplorer Server” on page 45
- ◆ “Configuration Summary for NetExplorer Manager” on page 55

Upgrading from ManageWise 2.5

If you upgrade from ManageWise 2.5, the NetExplorer software saves configuration information from the NXP.INI file to
SYS:\NMDISK\BACKUP\xxx\. Refer to this backed up information when you reconfigure NetExplorer using the NXPCON utility.

NetExplorer Console Configuration Utility

You can use the NXPCON utility on the NetExplorer Server to change the configuration for how NetExplorer runs; for example, the schedule and scope of discovery. You can also view the status of the initial discovery process.

To access the NXPCON utility

1. Access the server console on the NetExplorer Server.

You can access the NXPCON utility through the ManageWise Console, directly from the server prompt, or remotely.

In the ManageWise Console, select *Tools > Remote Console* to open a Remote Console window on the NetExplorer Server.

2. If the NetExplorer modules are already loaded on the server, select the *NetExplorer Console Utility* option in the Available Screens window.

Refer to “Step 1: Load the NetExplorer NLM Files” on page 42 for instructions for loading the NetExplorer NLM™ files for initial discovery.

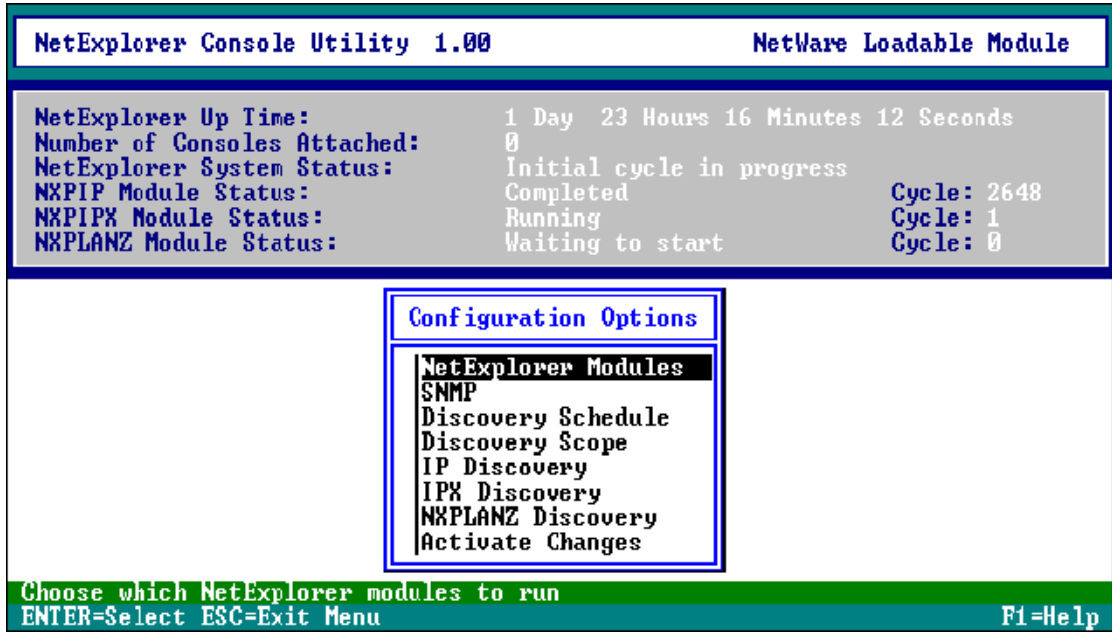
3. If the NetExplorer modules are not loaded, type the following at the server prompt.

```
Search Add SYS:\NMDISK
```

```
Load NXPCON
```

Figure 5-1 shows the NXPCON main window.

Figure 5-1
NetExplorer Console Utility Main Window



Task Overview

Table 5-1 provides a high-level view of the tasks you need to do to start discovery initially and customize the NetExplorer system to meet your organization's needs. Review the referenced sections for more detailed information about each of the tasks.

Table 5-1
Setup Task Overview

Setup Task	Required/Optional	Refer to
After ManageWise installation, start discovery.	Required	"Starting Discovery Initially" on page 42.
Check the status of initial discovery.	Recommended	"Checking the Status of Initial Discovery" on page 43.
Change NetExplorer Server configuration.	Optional	"Changing the NetExplorer Server Configuration" on page 45.

Table 5-1
Setup Task Overview

Setup Task	Required/Optional	Refer to
Change the NetExplorer Manager schedule.	Optional	"Changing NetExplorer Manager Settings" on page 55.

Starting Discovery Initially

Step 1: Load the NetExplorer NLM Files

Discovery starts automatically when NetExplorer software is loaded on the NetExplorer Server. To start the initial discovery process, do *either* of the following:

- ◆ Restart the NetExplorer Server to start NetExplorer.

When you restart your NetExplorer Server, NXPCON is launched by the LOAD SYS:\NMDISK\NXPCON line in your NETXPLOE.NCF file. The NETXPLOE.NCF file is called from your AUTOEXEC.NCF file.

- ◆ Load the NetExplorer NLM files manually.

If you are loading the NLM files manually, load NETEXPLOE. This process also loads the NXPCON utility. (Figure 5-1 shows the NXPCON main window.)

You can make a number of configuration changes to control how discovery occurs. If you want to make those changes now, refer to "Changing the NetExplorer Server Configuration" on page 45.

Once started, NetExplorer runs as scheduled in the NXPCON utility. By default, NetExplorer runs continually, 24 hours a day.

Step 2: Start NetExplorer Manager

You must start NetExplorer Manager on the ManageWise Console so that it can receive the discovered data from the NetExplorer NLM files on the NetExplorer Server. To start NetExplorer Manager, restart the ManageWise Console after ManageWise software installation.

Let NetExplorer Manager run as long as necessary to build the baseline data in the ManageWise Console database. This helps to ensure complete information and maps. The length of time it takes to build a complete database depends on the size of your network. Very small networks might take one or two hours; very large networks (several thousand nodes) might require a day or two.

Note



Database writing activities occur in the background. ManageWise discovery of your network might take a longer time to finish when you are using your system. Therefore, we recommend that you allow NetExplorer Manager to run overnight or over a weekend.

Refer to “Checking the Status of Initial Discovery” on page 43 for information about how to determine whether the initial discovery is finished.

Checking the Status of Initial Discovery

As discovery progresses, your topology maps in the ManageWise Console reflect the discovery data passed to the ManageWise Console database. However, in a large network, it might take up to a day or two before the initial discovery is complete.

Note



If the NetExplorer Manager icon on the ManageWise Console is flashing intermittently, NetExplorer Manager is busy gathering discovery data.

The easiest way to determine whether initial discovery is complete is to use the NXPCON utility on the NetExplorer Server to look at the status of each NetExplorer module. Each module must complete at least one full cycle for a complete map to be drawn.

To view the discovery status, look at the discovery status fields at the top of the NXPCON screen (see Figure 5-2). Refer to “NetExplorer Console Configuration Utility” on page 40 for information about how to access this screen.

Figure 5-2
Top of the NetExplorer Console Utility
Screen

NetExplorer Console Utility 1.00		NetWare Loadable Module
NetExplorer Up Time:	1 Day 23 Hours 16 Minutes 12 Seconds	
Number of Consoles Attached:	0	
NetExplorer System Status:	Initial cycle in progress	
NXPIP Module Status:	Completed	Cycle: 2648
NXPIPX Module Status:	Running	Cycle: 1
NXPLANZ Module Status:	Waiting to start	Cycle: 0

NetExplorer System Status indicates the overall status of the modules you selected to run by showing one of the following statuses:

- ◆ Initial cycle in progress—One or more discovery modules did not yet complete its first cycle.
- ◆ Initial cycle complete—All discovery modules completed at least one cycle.

NXPIP Module Status, *NXPIPX Module Status*, and *NXPLANZ Module Status* indicate the status of the modules by showing one of the following statuses:

- ◆ Not loaded—Indicates the module is not loaded. If you want to load the module, use NXPCON as described in “Changing Which NetExplorer Modules Are Loaded” on page 45.
- ◆ Waiting to start—Indicates that the module is loaded but has not started. NetExplorer modules run one at a time during initial discovery
- ◆ Completed—Shows how many cycles were completed.
- ◆ Running—Shows which cycle started

Changing the NetExplorer Server Configuration

Configuration Summary for the NetExplorer Server

Table 5-2
NetExplorer Server Configuration Summary

Situation	Configuration Task
You are not using TCP/IP in your network.	(Optional) You can configure NXPCON to not load the NXPIP module because it is unnecessary. Refer to "Changing Which NetExplorer Modules Are Loaded" on page 45.
Your organization uses SNMP community names other than "public."	Reconfigure SNMP community names. Refer to "Changing SNMP Community Names" on page 47.
You do not want to use the default discovery scope, which is all IPX™ networks in your internetwork and all IP routers in the same IP subnet as your NetExplorer Server.	Reconfigure the scope of discovery. Refer to "Changing the Discovery Scope" on page 48.
You do not want the NetExplorer NLM files to run continually on your NetExplorer Server.	Set the discovery schedule to specific days and times. Refer to "Changing the Discovery Schedule" on page 51.

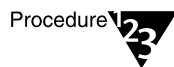
Changing Which NetExplorer Modules Are Loaded

By default, ManageWise installation loads the NXPCON utility with all modules running. If you are *not* using TCP/IP in your network, you can configure NXPCON to not load the NXPIP module because it is unnecessary. Otherwise, we recommend that you load all NetExplorer modules.



Note If you are using TCP/IP, TCP/IP must be bound to at least one of your server's network boards.

To view or modify which modules are being loaded



1. In NXPCON, select **NetExplorer Modules** from the **Configuration Options** menu

The NetExplorer Modules dialog box shown in Figure 5-3 appears.

Figure 5-3
NetExplorer Modules Dialog Box

NetExplorer Console Utility 1.00		NetWare Loadable Module
NetExplorer Up Time:	0 Day 4 Hours 25 Minutes 12 Seconds	
Number of Consoles Attached:	0	
NetExplorer System Status:	Initial cycle in progress	
NXPIP Module Status:	Not loaded	Cycle: 0
NXPIPX Module Status:	Running	Cycle: 1
NXPLANZ Module Status:	Waiting to start	Cycle: 0

Configuration Options

NetExplorer Modules

Use NXPIP? Yes

Use NXPIPX? Yes

Use NXPLANZ? Yes

NetExplorer Modules

NMP

discovery Schedule

discovery Scope

P Discovery

PX Discovery

NXPLANZ Discovery

Activate Changes

NXPIP discovers IP networks
ENTER=Select ESC=Previous Menu
F1=Help

2. **Select the field you want to change, and then press Enter.**
 A dialog box appears for the module that you selected.

3. **Select Yes or No to load or unload the module, and then press Enter.**
 You can either press Y or N or toggle between Yes and No using the Up-arrow and Down-arrow keys. The dialog box disappears and your selection appears in the NetExplorer Modules dialog box.

4. **Press Esc to exit the NetExplorer Modules dialog box.**
 A dialog box appears asking whether you want to save your changes.

5. **Select Yes.**

6. **Press Esc to exit NXPCON.**

7. **At the ManageWise Server prompt, enter the following command:**

UNXP

This command unloads the NetExplorer modules in the correct order.

8. At the ManageWise Server prompt, enter the following command:

NETXPLO

This command reloads the NetExplorer modules at the System Console prompt. Otherwise, restart your ManageWise Server for changes to take effect.

Changing SNMP Community Names

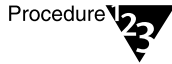
The default community name is “public.”



Note

If you have any LANtern™ nodes in your environment, note that their default community name is “administrator” instead of “public.” You need to change the community name on all LANtern nodes before they can be connected.

To view, add, modify, or delete SNMP configuration information, such as community names used for IP and IPX discovery



Procedure

1. In NXPCON, select **SNMP** from the Configuration Options menu.
2. In the SNMP dialog box, select **Edit Community Name List**.
3. To view, add, modify, or delete a community name
 - ◆ Press Insert to add a community name.
 - ◆ Select the community name you want to modify or delete, and then press Enter to modify or press Delete to delete.
4. Press Esc, and then select **Activate Changes** from the Configuration Options window.

Respond to the prompts accordingly.

For information about other configuration options in the SNMP window, refer to NXPCON online Help (F1) and *ManageWise 2.6 Network Management Guide*.

Changing the Discovery Scope

By default, NXPCON is set for discovery of all IPX networks in your internetwork and all IP routers in the same IP subnet as your NetExplorer Server. Using NXPCON, you can change the scope of what NetExplorer discovers. For IPX networks, you can limit the scope. For IP subnets, you can extend the scope.

You could, for example, limit discovery to only the IPX addresses you set NetExplorer to discover and the IP subnet addresses you configure. If you only monitor a section of a large network, you might want to limit discovery to that section, which would reduce traffic to parts of your network or make your maps more manageable.

After initial discovery, nodes remain in the ManageWise database until you reset the database, even if they have been removed from the network. If you limit discovery scope after initial discovery, you must reset the ManageWise database to remove the nodes that you no longer want in your database.

Note



If you change the discovery scope, you must also unload and reload NetExplorer NLM files on the NetExplorer Server and reset the database. If you do not, segments outside of the scope might appear on ManageWise maps. For more information, refer to *ManageWise 2.6 Network Management Guide* or to the ManageWise Console online Help.

Hints to Ensure Complete Discovery

IPX workstations are discovered with a username if the user is logged in to or attached to a server running NetWare® Management Agent™ software. To ensure that the usernames for IPX devices and workstations on your network can be discovered, install NetWare Management Agent on all NetWare servers where users log in.

If you have AppleTalk* devices that you want NetExplorer to discover, you need to install the NetWare LANalyzer Agent™ software on one server on each segment.

Changing the IP Discovery Scope

To view, expand, or restrict IP scope

Procedure



1. In NXPCON, select **Discovery Scope > IP Discovery Scope** from the Configuration Options window.

2. Press Enter to view or configure the scope of your discovery.

3. Perform one of the following steps:

- ◆ Press Insert to add a new IP discovery scope entry.

The Add Discovery Scope dialog box is displayed.

- ◆ Press Enter to modify a discovery scope entry.

- ◆ Press Delete to delete a discovery scope entry.

You can expand or restrict the scope of IP discovery by entering the IP address ranges specified by the mask fields you want to discover.

Restrict the scope by entering the IP address of your local network, together with the mask you want to use. You might want to specify the subnet mask of the subnet to which you are connected if you want to discover only this subnet.

The mask indicates what part of the address needs to match for discovery to proceed on a network segment. If you entered a number in the mask, the corresponding number in the IP address must match. A number 0 (zero) means that no match is required.

For example:

IP address: 10.5.0.0 and Mask: 255.255.0.0 allows discovery to proceed for any segment with an IP address starting with 10.5. NetExplorer discovers IP addresses 10.5.0.0 through 10.5.255.255.

If you do not specify a mask, the default mask, based on the network number class, is used.

4. Enter the address and mask (optional) for your discovery scope.

5. Press Esc, then select Yes to save changes to the configuration file.

6. Press Esc to return to the Discovery Scope window.

7. Unload and reload the NetExplorer modules, or restart your ManageWise Server, for changes to take effect.

8. To unload NetExplorer, enter the following command at the ManageWise Server prompt:

UNXP

This command unloads the NetExplorer modules in the correct order.

9. **Reload the NetExplorer modules by entering the following command at the server prompt:**

NETXPLO

This command loads NetExplorer and the NetExplorer modules in the correct order.

Changing the IPX Discovery Scope

To view, expand, or restrict IPX scope

Procedure



1. In NXPCON, select *Discovery Scope > IPX Discovery Scope* from the Configuration Options window.
2. Press Enter to view or configure the scope of your discovery.
3. Perform one of the following steps:
 - ◆ Press Insert to add a new IPX discovery scope entry.
The Add Discovery Scope dialog box is displayed.
 - ◆ Press Enter to modify a discovery scope entry.
 - ◆ Press Delete to delete a discovery scope entry.

You can expand or restrict the scope of IPX discovery by entering the IPX network numbers and the mask you want to use during discovery.

Restrict the scope by entering the IPX networks to be discovered by entering a single IPX network number and a mask. The mask indicates what part of the network number needs to match in order to match a discovered network. F in the mask means that the corresponding digit must match; 0 (zero) means that no match is required.

For example:

Network number: 12340000 and Mask: FFFF0000 matches any network number starting with 1234.

Network number: C00000FF and Mask: FF0000FF matches any network number starting with C0 and ending with FF, such as C01234FF, C00000FF.

4. **Enter the address and mask (optional) for your discovery scope.**
5. **Press Esc, then select Yes to save changes to the configuration file.**
6. **Press Esc to return to the Discovery Scope window.**
7. **Unload and reload the NetExplorer modules, or restart your ManageWise Server, for changes to take effect.**
8. **To unload NetExplorer, enter the following command at the ManageWise Server prompt:**

UNXP

This command unloads the NetExplorer modules in the correct order.

9. **Reload the NetExplorer modules by entering the following command at the server prompt:**

NETXPLO

This command loads NetExplorer and the NetExplorer modules in the correct order.

Changing the Discovery Schedule

You can configure the discovery schedule to run continually or periodically. By default, NetExplorer runs continually on the server. By running continually, NetExplorer detects any changes that might occur in your internetwork.

There are situations when you might not want to run NetExplorer continually. For example,

- ◆ If you want every node on the network discovered, schedule discovery during working hours when users are logged in.
- ◆ After you have an initial database of all nodes, run NetExplorer at off times to update the ManageWise database.

Once a node is in the database, it remains until you reset the database even if the node is removed from the network.

- ◆ Run NetExplorer periodically to reduce network traffic, especially over slow links or dial-up links.
- ◆ On a large network, run NetExplorer during hours when server utilization is low to minimize impact on system resources.
- ◆ On a large network, you might schedule NetExplorer to run over a lunch hour, or only at certain hours of the day when users are logged in but server utilization is low. Or, you might want to schedule NetExplorer to run only one cycle to free your server during hours when utilization is high.

Consider your network needs and resources when determining the NetExplorer discovery schedule.

Note



You can also schedule when you want to run NetExplorer Manager. For information about scheduling NetExplorer Manager, refer to “Configuring the NetExplorer Manager Schedule” on page 55.

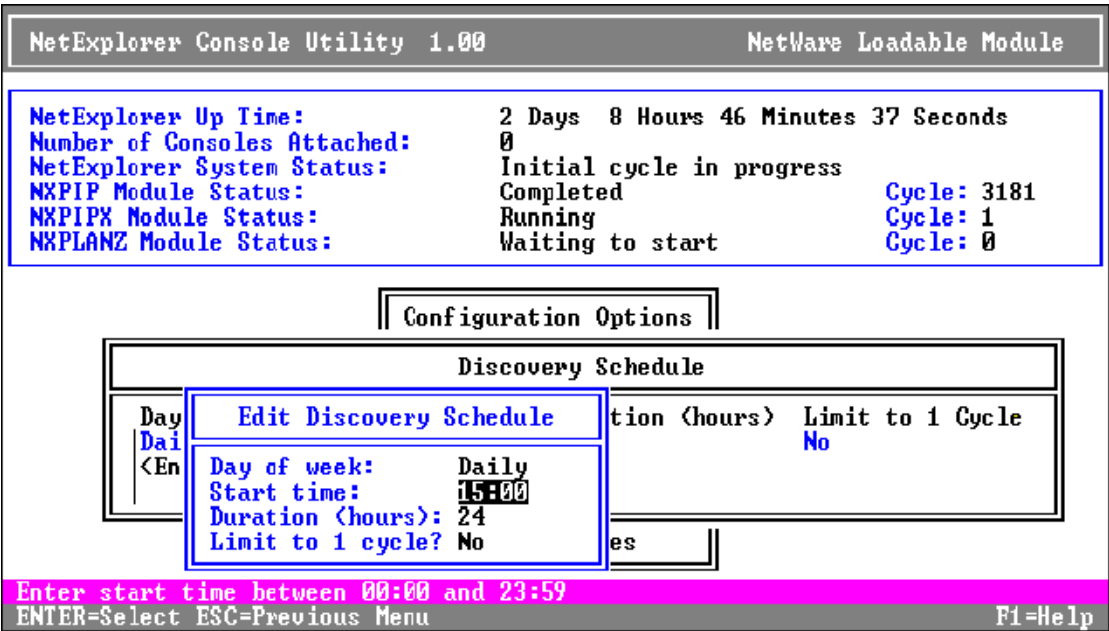
To view, modify, add, or delete a discovery schedule

- 1. Access NXPCON from your ManageWise Server or run RCONSOLE from your ManageWise Console.**
- 2. Select the NetExplorer Console Utility option in the Available Screens menu.**
- 3. Select *Discovery Schedule* from the Configuration Options window.**

The Edit Discovery Schedule dialog box is displayed.

Figure 5-4 shows NXPCON, Configuration Options, Discovery Schedule, and Edit Discovery Schedule windows that you use to view, modify, add, or delete a NetExplorer discovery schedule.

Figure 5-4
Edit Discovery Schedule Dialog Box



4. Perform one of the following steps:

- ◆ Press Insert to add a new schedule.
The Add Discovery Schedule dialog box is displayed.
- ◆ Press Enter to edit a schedule.
- ◆ Press Delete to delete a schedule.

5. Set your options.

- ◆ Set your NetExplorer discovery schedule for Daily, or select any day of the week in the Day of week field.

- ◆ Enter the time, in 24-hour format, you want NetExplorer discovery to begin in the Start time field. For example, enter 14:00 for 2:00 p.m.
- ◆ Enter the length of time, in hours, you want NetExplorer to run in the Duration (hours) field. The range is 1 hour to 168 hours (1 week).
- ◆ Specify *Yes* or *No* in the Limit to 1 cycle field. If you limit your NetExplorer discovery to 1 cycle, each discovery module (NXPIP, NXPIPX, and NXPLANZ) stops when it completes one discovery cycle of your network. If you do not limit discovery to one cycle, each module runs continually during the length of time you specified in the Duration (hours) field.



If the length of time you set in the Duration (hours) field is too short, not all modules have time to complete a cycle.

6. Press Esc, and then select *Activate Changes* from the Configuration Options window.

Respond to the prompts accordingly.

Loading and Unloading NetExplorer NLM Files

- ◆ To unload NetExplorer, enter the following command at the ManageWise Server prompt:

UNXP

This command unloads the NetExplorer modules in the correct order.

- ◆ To reload the NetExplorer modules, enter the following command at the server prompt:

NETXPLO

This command loads NetExplorer and the NetExplorer modules in the correct order.

- ◆ Unloading and reloading NETXPLO.NLM results in restarting the discovery process.

Changing NetExplorer Manager Settings

NetExplorer Manager on the ManageWise Console communicates with NetExplorer on the ManageWise Server to obtain network discovery data. Upon NetExplorer Manager's request, NetExplorer downloads discovered data to your ManageWise Console.

The first time NetExplorer Manager runs on the ManageWise Console, it begins writing to the database all the network information that NetExplorer found during the initial discovery cycle.

After the initial discovery, you can close NetExplorer Manager or continue to let it run in the background. Even if you close NetExplorer Manager, you should run it periodically to update the database.



Note NetExplorer continues to run on the ManageWise Server even if you stop NetExplorer Manager.

Configuration Summary for NetExplorer Manager

Table 5-3
Configuration Summary for NetExplorer Manager

Situation	Configuration Task
You do not want NetExplorer Manager running continually on the ManageWise Console.	On the ManageWise Console, set the NetExplorer Manager schedule. Refer to "Configuring the NetExplorer Manager Schedule" on page 55.

Configuring the NetExplorer Manager Schedule

After ManageWise software installation, NetExplorer Manager starts automatically after you restart Windows. By default, NetExplorer Manager runs continually.

Running NetExplorer Manager continually is useful if you want to generate a complete internetwork map that includes user login names. However, this uses the ManageWise Console resources continually as well. Therefore, you might want to consider the following other options for running NetExplorer Manager.

- ◆ Run it only at certain times of the day, each day. This frees resources on your ManageWise Console if you need to run other applications.
- ◆ Run it only at night or only on demand, when your ManageWise Console is not being used.

Note



If NetExplorer Manager is set to run continually, the NetExplorer Manager appears on your startup bar each time you start Windows.

To configure the NetExplorer Manager schedule

Procedure



1. **Start the ManageWise Console.**
2. **From the ManageWise Console window, select *Configure > Global Preferences*.**
3. **In the Global Preference dialog box, click the NetExplorer Options icon.**

The NetExplorer Options dialog box is displayed.

4. **In the NetExplorer Manager Calendar box, select the appropriate option button.**
 - ◆ To run NetExplorer Manager daily, select Run NetExplorer Manager Intermittently.
Enter a time for NetExplorer Manager to start, then select AM or PM. Then enter the number of minutes NetExplorer Manager is to run.
 - ◆ To run NetExplorer Manager whenever you have Windows open, select Run NetExplorer Manager Continually.
 - ◆ To run NetExplorer Manager only when you launch it, select Run NetExplorer Manager Only On Demand.

5. **Click Save.**

Any changes made take effect the next time you start ManageWise. NetExplorer Manager runs at the time you scheduled. It requires only that your PC be turned on, that the NetWare Client™ software be loaded, and that Windows be running.

Starting NetExplorer Manager Manually

If you want to start NetExplorer Manager at an unscheduled time, double-click the NetExplorer Manager icon in the ManageWise program group. NetExplorer Manager begins to communicate with NetExplorer and to add information to the database, as needed. If your network has changed very little since the previous update, it might take only a few seconds to complete.

Closing NetExplorer Manager

NetExplorer Manager runs in the background while you use ManageWise. During this time, you can run other applications on the console.

To close NetExplorer Manager

Procedure



- 1. Minimize the ManageWise Console window to display the ManageWise icons on the desktop.**
- 2. Click the NetExplorer Manager icon on the desktop, and then select Close.**
- 3. Return to ManageWise by double-clicking the minimized ManageWise Console icon.**

6 **Setting Up AntiVirus Protection**

This chapter briefly describes some of the tasks you might do in setting up anti-virus protection for your network. For detailed information, refer to the following manuals:

- ◆ *InocuLAN* Anti-Virus for NetWare* Supervisor's Guide*
- ◆ *InocuLAN 4 for Windows NT* Guide*
- ◆ *InocuLAN AntiVirus Guide*
- ◆ *InocuLAN AVUpdate Addendum*

To access these manuals, select the Online Manuals command in the ManageWise program group on the Windows Start menu.

The *InocuLAN AVUpdate Guide*, also accessible through the online manuals but is strictly for reference only. When InocuLAN is installed under ManageWise, setup is handled automatically.

Setting up InocuLAN for NetWare Server Software

InocuLAN for NetWare server software is installed from the ManageWise Installation program. Select the Custom Install setup option and check the InocuLAN for NetWare server software checkbox and follow directions given in the setup program.

Note



The option to install the InocuLAN for NetWare server software is only available on Windows 95 and Windows 98 consoles. When you install the ManageWise software on a Windows NT 4.0 workstation the this option is unavailable.

InocuLAN for NetWare Domain Manager

When InocuLAN is installed on the ManageWise Console workstation the InocuLAN for NetWare Domain Manager program is available from the ManageWise Console window. Select Cheyenne > Domain Manager to access the NetWare Domain Manager.

Note



The option to install the InocuLAN for NetWare server software is only available on Windows 95 and Windows 98 consoles. When you install the ManageWise software on a Windows NT 4.0 workstation the this option is unavailable.

Installing InocuLAN on a Windows NT Workstation

InocuLAN for Windows NT is provided in a separate installation program from the rest of ManageWise. You can access the InocuLAN for Windows NT install program from a link on the ManageWise CD-ROM splash screen or by running the SETUP.EXE program in the INOCULAN\WINNT\INTEL\CD\ directory on the ManageWise CD-ROM.

Note



InocuLAN for Windows NT contains two domain manager programs for Windows NT and NetWare. The Windows NT Domain Manager is the default domain manager, to manage NetWare domains you must select the NetWare domain manager checkbox in the Custom Install option when installing InocuLAN for Windows NT. For information about InocuLAN for Windows NT, refer to the "InocuLAN 4 Windows NT Guide."

To install virus protection for Windows NT systems,

1. **From a Windows NT 4.0 workstation, click the Install InocuLAN for Windows NT option on the splash screen that appears when you insert the ManageWise CD into the CD-ROM drive.**

You can also access the InocuLAN for Windows NT install program by running the SETUP.EXE program in the INOCULAN\WINNT\INTEL\CD\ directory on the ManageWise CD-ROM.

2. **Select Express Setup to install virus protection software on NT servers.**
3. **Select Remote Setup to install virus protection software on NT workstations.**

4. Select Custom Setup if your ManagageWise Console is on Windows NT.

5. Check the Install NetWare Domain Management Capability option.

Enabling this option allows you to manage virus protection on NetWare server domains.

For information about InocuLAN for Windows NT, refer to the “InocuLAN 4 Windows NT Guide.”

Possible Setup Tasks for AntiVirus Protection

After installing InocuLAN, some of the tasks you might want to do are as follows:

- ◆ Create an InocuLAN domain.

A domain is one or more InocuLAN servers (servers with InocuLAN Server software installed) that can share configuration and resources. You can, for example, set up one scan job that scans all the domain members. New virus signature files can be easily distributed to members of the domain.

- ◆ Schedule scans to occur automatically and at regular intervals.

- ◆ Customize the scanning process, including selecting file types to scan, the action to take if a virus is found, and skipping or including certain kinds of files.

- ◆ Provide users with information about how to install the complete InocuLAN functionality on their workstations. (The real-time monitor is installed automatically when the user logs into the InocuLAN Server.) Information about how to install InocuLAN on workstations is contained in Appendix C of the InocuLAN for NetWare Supervisor’s Guide.

Create an InocuLAN for Macintosh Install Disk

To install InocuLAN on a Macintosh computer, you need to create a Macintosh install diskette.

Creating a Macintosh Install Diskette

To create a Macintosh install diskette you will need to insert the ManageWise 2.6 CD-ROM in the ManageWise Console.

Procedure



1. From the Start menu select Run...
2. Browse the ManageWise 2.6 CD-ROM to the following path:

`\INOCULAN\CLIENTS\MAC\DISK1\INOMAC.EXE`
3. Run the INOMAC.EXE file.
4. A DOS box appears, insert a blank high-density diskette in drive A:> and press Enter.
5. The diskette is formatted into MAC O/S and the InocuLAN for Macintosh program files are copied to the diskette. The install diskette can be used to install directly on a Macintosh computer.

chapter 7 *Initial Setup in the ManageWise Console*

This chapter discusses the required and optional setup tasks that you do in the ManageWise® Console. Table 7-1 (tasks for the first few days) and Table 7-2 (tasks for the first few weeks) provide a quick reference to those tasks. Information about those tasks is included in this chapter.

Task Overview

Table 7-1
Setup Overview, First Few Days

Setup Task	Comments/Refer to
Set up security	
◆ Set up ManageWise Console security.	◆ Required if you want password protection for changes affecting the database. Refer to “Setting Up ManageWise Console Security” on page 64.
◆ For the desktop management component, edit a default security template for Windows 3.x, Windows 95 and Windows 98.	◆ Optional. Useful if, for example, you want to restrict access to add programs and directories that can be broadcast to all the workstations on the network. Refer to “Editing a Default Security Template for Chat or File Transfer” on page 65.
◆ For the desktop management component, set security options for Windows NT, and DOS workstations	◆ Refer to “DOS Security” on page 66. Refer to “Windows NT Security” on page 66
Enable segment alarms.	Required if you want to receive network alarms. Refer to instructions in the ManageWise Console online Help. (Search/Index keyword: segments, enabling alarms for.)
Assess whether the scope of discovery is correct.	Optional. Refer to “Refer to the “Desktop Management Guide” for detailed information on workstation security settings..”
Evaluate the NetExplorer™ Manager schedule.	Optional. Refer to “Configuring the NetExplorer Manager Schedule” on page 55.

Table 7-2
Setup Overview, First Few Weeks

Setup Task	Comments/Refer to
Change alarm thresholds for nodes and network segments.	Optional. Refer to “Changing Alarm Thresholds” on page 70.
Change default dispositions for how ManageWise is to handle alarms.	Optional. Refer to “Changing Default Alarm Dispositions” on page 69.
Create baseline documents to provide a record of typical activity on your network.	Optional. Refer to “Creating Baseline Documents” on page 71.
Create a custom map, for example, to show critical nodes.	Optional. Refer to “Creating a Custom Map of Critical Nodes on the Network” on page 71.
Add additional information to the ManageWise database to simplify your management tasks.	Optional. Refer to “Adding Additional Details to the ManageWise Database” on page 72.

Setting Up ManageWise Security

The following three security setup tasks are done in the ManageWise Console

- ◆ “Setting Up ManageWise Console Security.” (Optional)
- ◆ “Editing a Default Security Template for Chat or File Transfer.” (Optional)

Also refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide* for information about setting up security for secure SNMP transactions.

Setting Up ManageWise Console Security

You can set up password protection to prevent unauthorized users from accessing the following ManageWise Console functions that modify the database.

- ◆ Configuring servers and other objects
- ◆ Deleting objects

◆ Using the SNMP MIB Browser

◆ Changing a map

After you set a password, you must use it to log in to the ManageWise Console before you can perform any of these operations.

Setting the ManageWise Console Password

To set or change the ManageWise Console password

Procedure



1. In the ManageWise Console, select **Security > Change Console Password**.

The Change Console Password dialog box is displayed.

2. If a password exists, enter it in the Old Password field; otherwise, continue to Step 3.
3. Enter your new password in the New Password field.
4. Enter your new password again in the Confirm New Password field.

Logging In to the ManageWise Console

To log in to the ManageWise Console after you have set a password

Procedure



1. In the ManageWise Console, select **Security > Console Login**.

The Console Login dialog box is displayed.

2. Enter your password.

Editing a Default Security Template for Chat or File Transfer

During installation, ManageWise creates a default security template for use with Chat or File Transfer in Windows 3.x, Windows 95, and Windows 98 environments. Security settings are required to control the security for desktops that are on a network.

You can edit a default security template for each server or organizational unit. For example, you can add programs and directories that you do not want everyone to be able to access and broadcast to all

the workstations on the network. You can also create individual templates for users.

In a NetWare 3.x environment, the default template is given to all users who use the server as their primary server, but do not have an individual or remote template defined on the server. In a NetWare 4.x and NetWare 5 environment, the default template is defined within organizational units (OU). If an OU does not have a default template defined, it inherits the default template from the OU above it.

For information about editing the ManageWise Server default security template and creating individual security templates, follow the instructions for setting security parameters in the *ManageWise 2.6 Desktop Management Guide*.



The ManageWise Server default security template can be modified only when logged in to the network with SUPERVISOR (NetWare 3.1x) or ADMIN (NetWare 4.1x or NetWare 5) equivalent trustee rights.

DOS Security

The configuration program for DOS workstations(DOSCFG.EXE) copies the file, LDCLIENT.INI under the MWCLIENT directory on the workstation. You can edit this file to set the security parameters such as allowing access or permission required.

Sample LDCLIENT.INI file is as follows:

[SIGHT]

VISIBLE SIGNAL=YES

AUDIBLE SIGNAL=NO

PERMISSION REQUIRED=NO

Refer to the “Desktop Management Guide” for detailed information on workstation security settings.

Windows NT Security

The level of access for Windows NT workstations can be controlled using the Agent Security utility (EDTININT.EXE) under the MANAGEWISE group by the logged in user. The Agent Security utility

is installed on the Windows NT workstations when it is configured for ManageWise. This utility enables you to select or deselect the management features to be allowed on the Windows NT workstations.

The following table describes the parameters available for Windows NT workstations.

Table 7-3:
Security Parameters for Windows NT workstations

Parameter	Description
Remote Control	Enables control of the workstation.
Remote Reboot	Enables reboot of the workstation.
Remote File Transfer	Enables file transfer to and from the workstation's local drives.
Chat	Enables chat with the workstation.
Remote Execute	Enables program execution on the workstation.
Ping Test	Enables test of the workstation's network performance by sending network packets to the station as fast as possible.
Audible Signal	Enables alert sound every 10 seconds while the workstation is being accessed.
Visible Signal	In a client workstation while the workstation is being accessed, a display icon appears which can be enabled or disabled.
Permission Required	Enables confirmation from the user, before operator can access the remote workstation.

Refer to the “Desktop Management Guide” for detailed information on workstation security settings.

Checking the Results of Discovery

After NetExplorer Manager has finished updating the ManageWise database after initial discovery, we recommend that you check your maps to determine whether your network topology is represented on the maps as you expect.

If a node is not on the map, it might be of a type NetExplorer cannot discover. If a node does not appear in the correct segment, it might be because NetExplorer did not receive sufficient information to place it correctly. Refer to What NetExplorer Does and Does Not Discover in the ManageWise Console online Help. (Search/Index keyword: discovery, what NetExplorer discovers.)

You can manually add segments and nodes to your logical maps if NetExplorer cannot discover them, and make other corrections, as necessary. The information that you add is retained on your maps during future map updates. For instructions about editing your maps, refer to the *ManageWise 2.6 Network Management Guide* or the ManageWise Console online Help. (Search/Index keyword: maps, correcting.)

After your first maps accurately reflect your network, it is not necessary to regularly check the maps after NetExplorer Manager updates the ManageWise database. However, if you reset the ManageWise database or reset the network topology, we recommend that you check your maps again.

Evaluating the NetExplorer Manager Schedule

By default, NetExplorer Manager is set to run continually. This ensures that your ManageWise database is built as soon as possible after installation and that ManageWise maps and data windows remain up-to-date. After you are satisfied that your maps accurately reflect your network, you should evaluate whether running NetExplorer Manager continually best meets the needs of your organization.

Review the recommendations in “Configuring the NetExplorer Manager Schedule.” If desired, change the schedule as instructed in that section.

Setting Up Alarm Handling

ManageWise provides defaults to handle most aspects of alarm handling. After you have had some experience with your network, you might find that the default settings need to be adjusted. For example, you might not be receiving alarms as early as you want to be able to take preventive action for a problem.

Read the following sections:

- ◆ “Enabling Alarms” on page 69
- ◆ “Changing Default Alarm Dispositions” on page 69
- ◆ “Changing Alarm Thresholds” on page 70

Refer also to “Configuring NetWare Management Agent” on page 73 for information about other things you can do to affect alarm management.

Enabling Alarms

- ◆ By default, ManageWise enables alarms for NetWare servers and provides default alarm thresholds.
- ◆ By default, ManageWise *does not* enable segment alarms, although it does provide default threshold values for them. If you did not enable alarms as instructed in the Post-installation Help file, do it now. Otherwise, the ManageWise Console will not receive any network alarms. Refer to the ManageWise Console online Help for more instructions. (Search/Index keyword: segments, enabling alarms for.)

Changing Default Alarm Dispositions

ManageWise provides defaults, by alarm type, for the severity level assigned to the alarm, the operational state of the object affected by the alarm condition, and the disposition of the alarm (for example, whether ManageWise logs the alarm to the database or displays the alarm as a ticker-tape message in the ManageWise Console window). You might want to change the ManageWise defaults to match your preferences. For example, you might consider an alarm less severe than the defaults attributed to it or you might want to log the alarm to the database even though it is not, by default.

You can view all alarms and their default alarm disposition in the Alarm Disposition Table window (select *Fault > Alarm Disposition*). For instructions about how to change the disposition, refer to the ManageWise online Help. (Search/Index keyword: disposition, changing.)



For details about a particular alarm, select the alarm in the Alarm Disposition Table and then click the NetWare Expert™ button.

Changing Alarm Thresholds

Over the first few weeks, evaluate whether too many or not enough alarms are being generated on your network to alert you to atypical conditions. Then change the alarm threshold values as appropriate.

- ◆ For alarms generated by NetWare servers, you change alarm thresholds on a server by server basis, either through the ManageWise Console or by reconfiguring files on that server.
- ◆ Changes you make through the ManageWise Console to alarm threshold settings are not written to the NTREND.INI file. Therefore, should you want to return to the default settings provided by ManageWise, you can do so by loading NTREND.NLM with the Reset option.

For instructions about changing alarm thresholds through the ManageWise Console, refer to the *ManageWise 2.6 Network Management Guide* or the ManageWise Console online Help (Search/Index keyword: alarm thresholds, setting for a server)

- ◆ Editing the NTREND.INI file directly results in those settings becoming the default settings. You cannot return to the default settings provided by ManageWise unless you save a copy of NTREND.INI.

For instructions about reconfiguring files on the NetWare Management Agent Server, refer to the *NetWare Management Agent 2.6 Installation and Configuration* guide.

- ◆ For alarms generated by NetWare LANalyzer® Agent™ software, you change alarm thresholds on a segment by segment basis through the ManageWise Console. Refer to the *ManageWise 2.6 Network Management Guide* or the ManageWise Console online Help (Search/Index keyword: alarm thresholds, setting for a segment).

Additional Tasks to Enhance Network Management

There are several optional tasks that you can do that make enhance your network management capabilities.

- ◆ “Creating Baseline Documents” on page 71
- ◆ “Creating a Custom Map of Critical Nodes on the Network” on page 71
- ◆ “Adding Additional Details to the ManageWise Database” on page 72

Creating Baseline Documents

Creating baseline documents of normal activity of various nodes and network segments provides valuable information when you are troubleshooting a problem. If you know what normal activity of a node or segment is, you can then determine when the activity is not normal. ManageWise provides real-time and trend data, captured at various intervals, which gives you a good history of segment and server activity.

For more information, refer to the ManageWise Console online Help. (Search/Index keyword: baseline documents.)

Creating a Custom Map of Critical Nodes on the Network

You might want to create maps of your network that show exactly what you want to see. For example, you might want to create a map that shows critical segments or nodes so that you can quickly recognize any problems with those nodes. (When a node generates an alarm of critical, major, or minor severity, ManageWise displays an alarm bell on a map next to the node.)

For more information, refer to the ManageWise Console online Help. (Search/Index keyword: custom maps, creating.)

Adding Additional Details to the ManageWise Database

You might want to have easy access to details about a node or segment that are not provided by the discovery process. For example, you might want to have quick access to physical information about a server (such as its disk size, CPU model, RAM size, and so on), or who to contact in case of a problem with a node or segment. You can manually add this and other information through the Database Object Editor. You might also want to use this editor to edit some of the data provided by NetExplorer; for example, to change the segment name to be one that is more meaningful to you.

For more information, refer to the *ManageWise 2.6 Network Management Guide* or the ManageWise Console online Help. (Search/Index keywords: Database Object Editor, using to add details about a node; Database Object Editor, using to add details about a segment.)

8 **Configuring ManageWise Agents**

This chapter summarizes configuration tasks for NetWare® Management Agent™ software and NetWare LANalyzer® Agent™ software. A separate detailed guide is provided for each of these agents as part of the ManageWise® online documentation.

ManageWise Setup installs these agents on the ManageWise Server. You might also install these agents as standalone products on non-ManageWise Servers.

Default configurations are provided so you can immediately view data from these agents in your ManageWise Console. These defaults are sufficient for most organizations. However, after you have evaluated the data you are receiving, you might want to change the default settings to meet your organization's needs.



Note

Each of the agent manuals contains a chapter about installing the agent. Read the installation chapter only if you are installing the agent as a standalone application.

Configuring NetWare Management Agent

Each server that you want to manage through the ManageWise Console must have NetWare Management Agent installed. After NetWare Management Agent is installed on a server, the agent is ready to operate in its default state. In most cases, the default state is sufficient for operation. However, you can customize NetWare Management Agent.

This section summarizes how you can change the default settings for your environment. For details, refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide*.

Task Overview for NetWare Management Agent Configuration

Optional configuration tasks related to NetWare Management Agent are shown in the following list:

- ◆ “Changing Security Settings for SET and GET Operations” on page 74
- ◆ “Changing NLM File Load Parameters” on page 75
- ◆ “Changing Alarm Threshold Values in NTREND.INI” on page 75
- ◆ “Changing Trend Values in NTREND.INI” on page 75
- ◆ “Controlling How Alarm Generation Occurs” on page 76
- ◆ “Sending Alarms to non-ManageWise Management Stations” on page 76
- ◆ “Limiting Transmission of SAP Packets from ManageWise Consoles” on page 77

Changing Security Settings for SET and GET Operations

When NetWare Management Agent is initially installed on the server, the default security settings are as follows:

◆ SET requests

The default setting is SNMP packets over the NetWare Core Protocol™ (NCP™) protocol, which requires SUPERVISOR or OPERATOR privileges to issue SET requests to the server.



SNMP over NCP is more secure than security handled only through community names because it encrypts passwords.

◆ GET requests

By default, the community name for the SNMP Monitor community parameter (which allows GET requests) is set to “public.” A user without SUPERVISOR or OPERATOR privileges can obtain data, as long as the console from which the user is issuing the command and the NetWare Management Agent Server

have the same community name set for the MonitorCommunity parameter.

Community names are case sensitive. The community name must be “public.” It cannot be “Public” or “PUBLIC.”

Read the description of available security options in the *NetWare Management Agent 2.6 Installation and Configuration Guide* to determine how you want to set up security. Procedures for configuring each of the security options is included.

Changing NLM File Load Parameters

When the NetWare server is started, the NMA2.NCF (NetWare 3.1x & NetWare 4.1x) or NMA5.NCF (NetWare 5) automatically loads all the NLM™ files required for NetWare Management Agent in a default configuration state. You can configure LOAD parameters for each of the NLM files used with the agent to control how the NLM file is loaded.

Refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide* for details about the LOAD parameters.

Changing Trend Values in NTREND.INI

The trend values in the NTREND.INI file specify the time interval (Sample Interval) at which a particular trend parameter is sampled, the duration of time for which those samples are kept (Trend Buckets), and whether this sampling parameter is enabled (Enbl).

The default settings should be sufficient to provide trend data for you initially. After ManageWise has been running for a while, you can evaluate whether the trend data being gathered is at the time interval and duration that you need.

Refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide* for specific information about how to change trend values.

Changing Alarm Threshold Values in NTREND.INI

For alarms generated by NetWare servers, you change alarm thresholds on a server by server basis, either through the ManageWise Console or by reconfiguring files on that server.

- ◆ Changes you make through the ManageWise Console to alarm threshold settings are not written to the NTREND.INI file. Therefore, should you want to return to the default settings provided by ManageWise, you can do so by loading NTREND.NLM with the Reset option.

For instructions for changing alarm thresholds through the ManageWise Console, refer to the *ManageWise 2.6 Network Management Guide* or the ManageWise Console online Help (Search/Index keyword: alarm thresholds, setting for a server)

- ◆ Editing the NTREND.INI file directly results in your settings becoming the default settings. You cannot return to the default settings provided by ManageWise unless you save a copy of NTREND.INI.

For instructions for reconfiguring files on the NetWare Management Agent Server, refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide*.

Controlling How Alarm Generation Occurs

By editing NWTRAP.CFG, the NWTRAP.NLM configuration file, you can control such things as

- ◆ Types of alarms NWTRAP.NLM forwards to management stations
- ◆ Time interval during which an identical alarm is sent
- ◆ Traps to be disabled
- ◆ Minimum severity level of alarms to be forwarded to management stations

Refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide* for details.

Sending Alarms to non-ManageWise Management Stations

ManageWise Consoles use the Service Advertising Protocol (SAP) to identify themselves to NetWare Management Agent software installed on NetWare servers. Thus, ManageWise Consoles automatically receive alarms.

You can manually add to the TRAPTARG.CFG file the addresses of other recipients who are to receive traps. This is useful for having traps sent to network management consoles other than the ManageWise Console and if you are using SAP filters in any of the routers on your network.

Refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide* for details.

Limiting Transmission of SAP Packets from ManageWise Consoles

Each ManageWise Console sends a SAP packet with the ID number 0x026a. FINDNMS.NLM uses this packet to identify consoles that it should send traps to. This process can create excessive traffic on remote links. This is a particular problem for on-demand, dial-up connections. For the procedure for how to eliminate this problem, refer to the *NetWare Management Agent 2.6 Installation and Configuration Guide*.

Configuring NetWare LANalyzer Agent

This section provides a summary of the tasks that you can do to configure NetWare LANalyzer Agent. Refer to the *NetWare LANalyzer Agent 1.21 Installation and Administration* guide for more information.

Task Overview for NetWare LANalyzer Agent Configuration

Optional configuration tasks related to NetWare LANalyzer Agent are shown in the following list:

- ◆ “Improving the Performance of NetWare LANalyzer Agent” on page 77
- ◆ “Enabling or Disabling Network Monitoring by Selected Network Adapters” on page 78

Improving the Performance of NetWare LANalyzer Agent

The LANZ.NCF file loads all the NLM software required for NetWare LANalyzer Agent operation. The LANZ.NCF file resides in the SYS:SYSTEM directory. You can improve the performance of NetWare LANalyzer Agent by modifying the LANZ.NCF file. Refer to the

NetWare LANalyzer Agent 1.21 Installation and Administration guide for more details.

Enabling or Disabling Network Monitoring by Selected Network Adapters

You only need to install one NetWare LANalyzer Agent on each segment. However, if you have multiple servers with NetWare LANalyzer Agent software installed, you might want to enable or disable network monitoring by network adapter in the following situations:

- ◆ You might want to switch because you want to monitor different segments.
- ◆ You might want to switch between agents on the same segment because maybe one agent is more efficient than the other (for example, in memory, disk space, or speed).
- ◆ You might want to switch because the agents are on the two sides of a repeater.

Refer to the *NetWare LANalyzer Agent 1.21 Installation and Administration* guide for instructions.

Installing Desktop Remote as a Standalone Application

Desktop Remote is installed on the ManageWise® Console during the ManageWise installation process and can be accessed through the menu bar. This chapter describes how you can also install Desktop Remote as a standalone application.

Introduction to Desktop Remote

Using asynchronous communication lines, Desktop Remote enables users to control Windows 3.x and Windows 95 workstations from remote locations by way of a modem.

- ◆ Network administrators can configure dedicated workstations to serve as hosts, providing authorized users access to the LAN by way of a modem.
- ◆ Users can completely control host workstations, precisely as they would over the LAN. Users can also transfer files back and forth between their own workstations and the host workstation.

Note



The Desktop Remote host mode functionality is not supported on Windows NT. You can dial into Windows* 3.x, Windows 95*, and Windows 98* workstations running in host mode from a Windows NT workstation.

Desktop Remote is an ideal tool for the following situations:

- ◆ Employees who travel frequently and need access to critical software and files stored on the office LAN.
- ◆ Network administrators who manage satellite networks and need to access them without traveling to the remote sites.
- ◆ Network administrators who set up their workstations as a host each night. If, during the night, administrators are required to

support users at the office, they can call in from their PC at home to the host at work.

Modem Requirements

Because Desktop Remote relies on modem communications, it is important that users understand how to use their modems. Desktop Remote is intended for use with Hayes*-compatible modems and can be used with many different brands of modem.

Because modem configurations vary widely, refer to the owner's manual for your modem to determine proper configuration settings.

Remote System Requirements

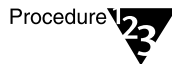
Desktop Remote requires the following computer hardware and software to function properly:

- ◆ 80386SX 16 MHz or faster IBM*-compatible PC
- ◆ 4 MB or more of system memory
- ◆ 1200 bus modem or better (14.4 kbps recommended)
- ◆ MS-DOS 5.0 or later
- ◆ Windows 3.x, Windows 95, Windows 98, Windows NT

Installing Desktop Remote as a Standalone Application

The following installation procedure installs Desktop Remote as a standalone application using SETUP.EXE, found in the LDT\DTREMOTE directory on the ManageWise CD-ROM.

To install Desktop Remote from the ManageWise CD-ROM



- 1. Insert your ManageWise CD-ROM into your CD-ROM drive.**
- 2. From Windows Program Manager, select *File > Run*.**
- 3. Enter the following command line:**

`DRIVE:LDT\DTREMOTE\SETUP.EXE`

where *drive* indicates the drive mapped to your CD-ROM.

- 4. Click OK.**
- 5. Follow the on-screen prompts.**
- 6. Click the Restart Now button after the installation is complete.**

Note



Rather than installing from the ManageWise CD-ROM, you can copy the files from the LDT\DTREMOTE directory to a single diskette. Then, run SETUP.EXE from the disk drive of your home computer.

Desktop Remote's Setup program restarts Windows after completing the installation. This activates the Windows device driver required to run Desktop Remote.

chapter **10** *Integrating Third-Party Applications*

This chapter provides an overview of how various third-party applications and integrated agents add functionality to your ManageWise® software. It also provides hints to help you be successful while installing third-party software to work with ManageWise.

Small-to-Medium Network Scenario

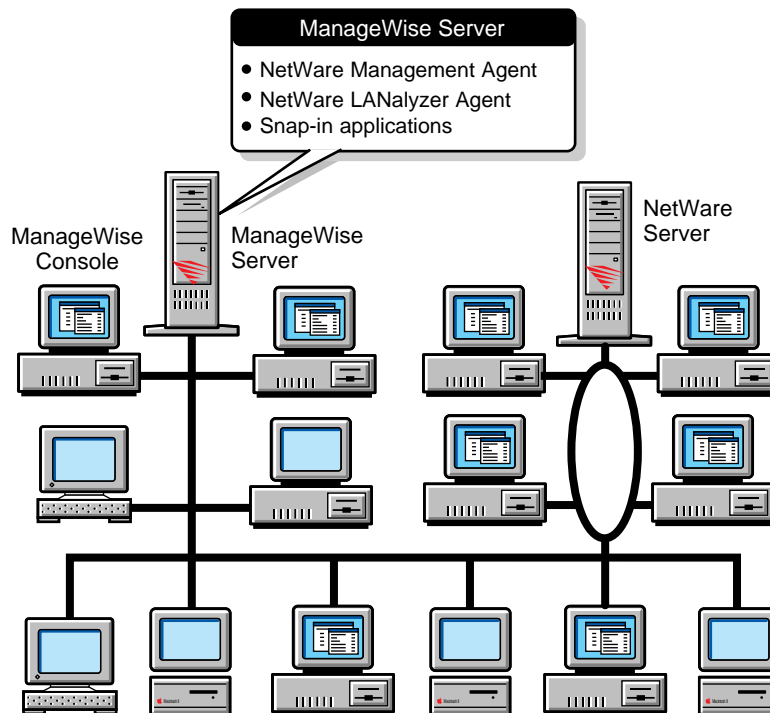
A typical small-to-medium network might involve several file servers, print servers, and 100 to 200 clients. Integrated agents, such as NetWare® LANalyzer® Agent™ software, NetWare Management Agent™ software, and third-party applications, add functionality and managing capabilities to ManageWise.

Some enhancements useful for a typical small-to-medium network enable you to perform the following tasks:

- ◆ Monitor disk, volume, and memory usage
- ◆ Monitor print status
- ◆ Set and monitor alarm thresholds on critical server parameters
- ◆ Acquire detailed performance statistics and trends for all traffic on a segment
- ◆ Detect network overload, excessive errors, and stations with duplicate IP addresses
- ◆ Receive remote notification by using a pager utility to forward network alarms to your alphanumeric pager or electronic mailbox based on the severity of the alarm
- ◆ Monitor the status of and troubleshoot client workstations remotely

Figure 10-1 shows a small-to-medium network using integrated agents.

Figure 10-1
Sample Integrated Agent Deployment on a
Small-to-Medium Network



Medium-to-Large Network Scenario

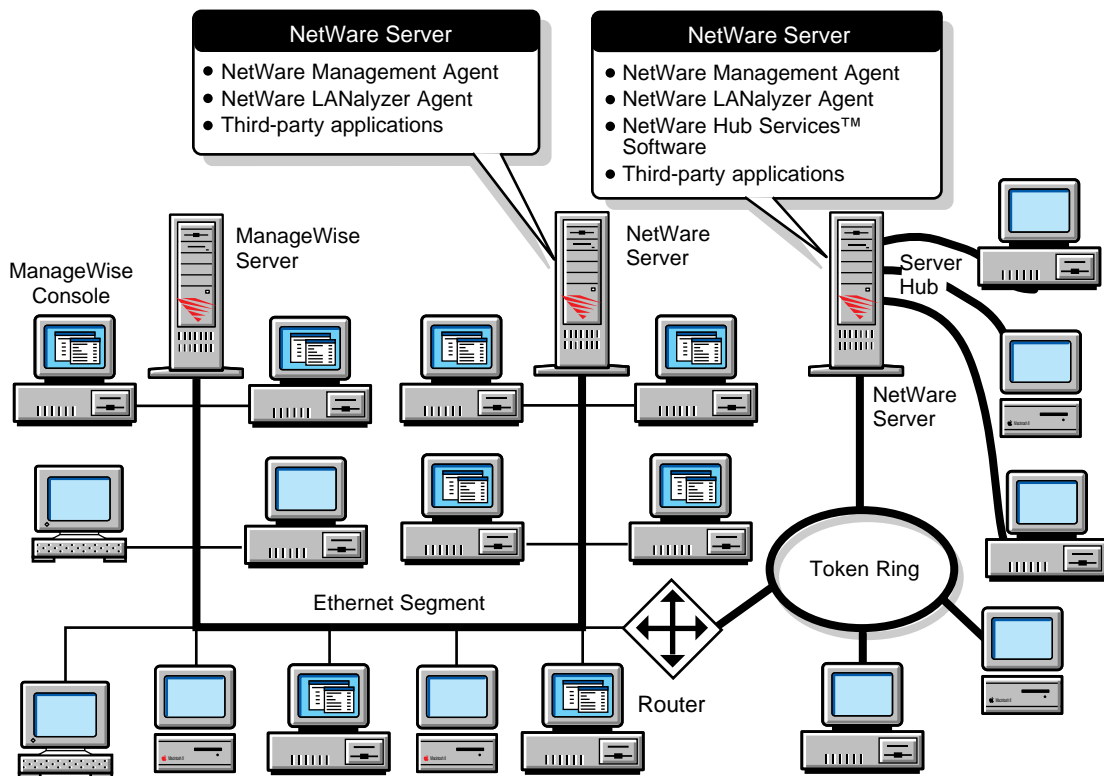
A typical medium-to-large network might involve a dozen file servers; many hubs, routers, and print servers; and 500 or more clients. Integrated agents, such as NetWare LANalyzer Agent, NetWare Management Agent, and so on, add functionality and managing capabilities to ManageWise. Some enhancements useful for a typical medium-to-large network include all the functionality listed for a small-to-medium network, as well as the following:

- ◆ View predictive analysis and be alerted to specific issues or impending problems
- ◆ Enable automatic corrective action before failures occur.

- ◆ Plan ahead to avert network problems, instead of reacting to unplanned down time.

Figure 10-2 shows integrated agents and third-party applications deployed to manage your medium-to-large network effectively.

Figure 10-2
Sample Integrated Agent Deployment on a
Medium-to-Large Network



What to Record about Third-Party Applications

Information that you want to record varies according to the application. The following are examples of information you might want to record:

- ◆ SNMP addresses and masks for each third-party device (UPC system, hubs, and so on).
- ◆ SNMP community strings (monitor, control, trap settings) defined for management access and security for each network device.
- ◆ Names and copies of MIB files added to ManageWise.
- ◆ Telephone number, e-mail address, and so on of the network administrator contact.
- ◆ Software version of applications added to ManageWise and where installed files were added. Some third-party applications add an install log during installation that saves this type of information.
- ◆ Contacts and technical support numbers for each application.
- ◆ Whether an asynchronous terminal is required to configure the device (hubs and power management systems, for example).

Prerequisites to Installing Third-Party Software

We recommend that you install any third-party applications and integrated agents after you install ManageWise. Following are several tasks to complete before you install any third-party applications or integrated agents:

1. Log information about third-party information. See “What to Record about Third-Party Applications” on page 86.
2. Back up the NMS.INI, WINDOWS.INI, and SYSTEM.INI files.
3. Back up the ManageWise database if you are concerned about maintaining network topology information. You can do this by using the Database Administration Tool.
4. Review your third-party application documentation.

Refer to your third-party documentation for more detailed information before installing and integrating third-party applications.

5. Verify that enough disk space exists to run the third-party application.

Third-Party Installation Hints

The following notes might help you if you are unfamiliar with a third-party application or if you experience a problem. If you cannot solve your problem, call the third-party technical support.

- ◆ When installing the third-party application, ensure that you install to \MW\NMS. Some third-party applications install to \NMS, which is not valid.
- ◆ Most third-party applications provide initialization documentation. Some vendors add a Windows program group and icon for user selection and execution. Other vendors hook directly to ManageWise and add selection items to the ManageWise drop-down menus.
- ◆ Verify that the third-party application is initialized during ManageWise startup and verify that the application can be started through icon selection or ManageWise launch.
- ◆ For devices that have an SNMP address, ping the device from the ManageWise Console to verify the network communication path. If you do not receive a response, you might have one of the following problems:
 - ◆ The device is not configured correctly for IP ping.
 - ◆ The device is not attached to the ManageWise local segment.
 - ◆ The router might not forward the IP ping request.
 - ◆ The SNMP monitor, control, or trap settings do not match the ManageWise settings. When the IP ping is sent, the device does not respond.
- ◆ Some applications automatically install MIB information that translates SNMP trap messages that they send. You should add this MIB information to the ManageWise MIB collection using the MIB Compiler.

- ◆ If you are viewing the Internetwork map and cannot find an icon for a third-party application that should be there, that third-party application probably implements its own discovery process. Refer to that third-party application documentation for more information.

Migrating Previously Installed Third-Party Software

If you are upgrading ManageWise and have third-party applications installed, you might need to compare the backup copy of your NMS.INI file to the new NMS.INI file to see whether any entries affecting previously installed software were changed.

A ***Troubleshooting Installation and Startup***

This chapter provides information to help you troubleshoot installation and startup of ManageWise® software. It is divided into the following sections:

- ◆ “Troubleshooting the ManageWise Server”
- ◆ “Troubleshooting the ManageWise Console”
- ◆ “Troubleshooting Desktop Management Problems”
- ◆ “Troubleshooting Your WAN Environment”
- ◆ “Technical Support and Update Information”

Troubleshooting the ManageWise Server

Problem: Server Halts (Abends)

If the server halts

Procedure



1. **Do *not* turn off your server.**
2. **Record the information displayed on the server console:**
 - ◆ Date and time the system halted.
 - ◆ Description of the problem, including the process that was running at the time the system halted.
 - ◆ Stack information at the time the system halted.

3. Restart the server, then enter the following system administration commands and record the information listed:

Command	Information to Record
MEMORY	Total server memory
VERSION	Version of NetWare® software
CONFIG	Server configuration information
LOAD MONITOR (to view server information and performance):	
DISK INFORMATION	Information listed in Monitor
DEVICE #0	Disk driver information listed in Monitor (for example ISADISK.DSK)
MODULES	Currently loaded NLM™ files

4. Call your reseller for ManageWise troubleshooting information.

Problem: Installation Cannot Copy .NCF Files

Explanation Occasionally during NetExplorer™ software installation, the error message “Unable to copy files AUTOEXEC.NCF or NMSBASE.NCF” appears.

Action If this message appears, follow these steps:

Procedure



1. Exit the ManageWise installation.
2. Exit Windows.
3. Log out of all servers.
4. Start Windows again.
5. Start the ManageWise installation again.

Reinstall the ManageWise Server software. Do not reinstall the ManageWise Console software.

Problem: Short-Term Memory Allocation Failures

	Your NetWare server software reports short-term memory allocation failures when running the discovery NLM files.
Explanation	The discovery NLM files require up to 8 MB of server RAM on large networks.
Action	<p>The discovery NLM files require up to 8 MB of server RAM on large networks.</p> <p>Other solutions might be to add more RAM or reduce the size of the receive buffers in your STARTUP.NCF file.</p>

Decreasing Memory on the ManageWise Server

The default ManageWise Server configuration reserves more memory than might be required in your environment. You can decrease memory consumption on your server by decreasing the values of the Maximum Packet Receive Buffers and Maximum Physical Receive Packet Size SET variables, as described in the following section.

Decreasing the Maximum Packet Receive Buffers

The NMSBASE.NCF file sets the maximum number of packet receive buffers to 500. Many environments do not require this large a number. Because a large number of buffers consumes more memory, you might want to decrease this number and verify that it does not cause problems. (The value should be between 100 and 500.) If you decrease the number and do not observe problems with your server that could be caused by dropped packets, keep the variable set to the smaller value. You can change the setting in the NMSBASE.NCF file; this file is located in the SYS:\SYSTEM directory.

Decreasing the Maximum Physical Receive Packet Size

NetWare uses 4,202 bytes as the default size; this value is required on token ring, but not on Ethernet. If your server is connected only to Ethernet segments, you can reduce this value to 1,518 bytes. The value must be specified in the STARTUP.NCF file, which resides on the DOS partition of your server. You can bring the server down, modify the value in the STARTUP.NCF file, and then bring the server back up. Alternatively, you can modify the STARTUP.NCF file using the Server Manager utility.

To modify the value in the STARTUP.NCF file

Procedure



1. At the ManageWise Server console, enter

`LOAD SERVMAN`

2. Select *Server Parameters* from the menu that appears.

3. Select *Communications* from the menu that appears.

4. Edit the value in the resulting screen.

Note



You must still restart the server for the change to take effect.

Troubleshooting NetWare LANalyzer Agent Software

This section provides information to help you solve problems you might encounter with NetWare LANalyzer® Agent™ software.

Receiving Token Ring Alarms

To receive token ring alarms on instrumented servers, make sure you are using a TOKEN.LAN driver file dated 09/09/91 or later.

IPX, Network Boards, and Segment Monitoring

NetWare LANalyzer Agent software requires at least one network board to be bound to the IPX™ protocol for the ManageWise Console to communicate with it. It does not require every network adapter to be bound to IPX or to another network protocol.

Note



A potential side effect of not binding IPX to each network board is that your internetwork map might have disjointed or “island” segment icons (on segments for which NetExplorer could not determine where they should be connected).

Changing Network Boards

If you change or add a network board that you want NetWare LANalyzer Agent to monitor

Procedure



1. At the ManageWise Server console, enter

`ULANZ`

2. From a workstation that is logged in with SUPERVISOR rights, delete the following file:

`SYS:\LANZ\LANZ.CFG`

3. At the ManageWise Server console, enter

`LANZ`

Problem: Inaccurate NetWare LANalyzer Agent Statistics

NetWare LANalyzer Agent is gathering and reporting inaccurate or unreliable statistics.

Explanation The LAN driver that you are using might not be correct for the network adapter you are using.

Action Verify that you are using the latest Novell-certified LAN driver for the network adapter you are using by pointing your browser to <http://developer.novell.com/devres/langrp/cards/cards.htm> or go to the Novell Labs Information System LAN Adapters and Drivers Index at http://developer.novell.com/infosys/mastr_02.htm. Updates to Novell® drivers are posted on the technical support site or at the NetWire® electronic bulletin board. For more information about how to obtain current updates, refer to “Technical Support and Update Information.”

Problem: Missing Bar Chart in the Network Dashboard Window

Explanation The bar chart is missing from the bottom portion of the Network Dashboard™ window.

Action Make sure that SNMP is loaded explicitly with the following parameters:

`LOAD SNMP VERBOSE CONTROL= TRAP=`

If you have this statement in your AUTOEXEC.NCF file, make sure that another NLM file isn't automatically loading SNMP without the parameters. To ensure that these parameters are being used, load CONLOG.NLM (in NOVLIB, Lib 9, CONLOG.EXE) to review the loading of the NLM files. When SNMP loads, it should return the following message:

SNMP: ControlCommunity now accepts any community name

Troubleshooting the ManageWise Console

This section provides information to help you solve problems with the NetWare Client™ software and the ManageWise Console.

Problem: Sluggish ManageWise Console

- | | |
|-------------|---|
| Explanation | During the initial discovery phase, the ManageWise software might be sluggish if you have a very large network and NetExplorer Manager is populating the database and writing to the disk. After the discovery process is complete, console performance improves. |
| Action | We recommend that you schedule NetExplorer Manager's initial discovery when you do not need your workstation, such as overnight or over a weekend. |

Problem: Internetwork Map Is Empty after ManageWise Runs for a While

For example, NetExplorer has been running for two hours and when you select *File > Open > Internetwork Map*, the map is empty.

To address this situation:

Procedure



1. **Use the NXPCON utility on the ManageWise Server to verify that NetExplorer NLM files are running on the server.**

This utility informs you of the NLM status.

2. **Check the Number of ManageWise Consoles field in NXPCON on your ManageWise Server.**

This value is incremented each time a new ManageWise Console attaches to the ManageWise Server. If this value is 0, it means that no ManageWise Console is attached to the ManageWise Server.

3. **If you receive the message, verify that NetExplorer Manager is running on your ManageWise Console.**

If a red circle hash symbol appears over the NetExplorer icon, it cannot connect with the ManageWise Server.

Problem: Incomplete Internetwork Map after ManageWise Runs for a While

For example, NetExplorer has been running for two hours and when you select *File > Open > Internetwork Map*, only some of your systems and networks are discovered.

To address this situation

Procedure



1. **In the NXPCON utility on the ManageWise Server, expand the scope set for IP discovery.**

By default, only the IP network to which your server is connected (as determined by the class of your IP address) is discovered. Refer to “Changing the IP Discovery Scope” for the procedure.

2. **Configure additional SNMP community names if some of your systems are using an SNMP community name other than “public.”**

Refer to “Changing SNMP Community Names” on page 47 for the procedure.

3. Use NXPCON to select *SNMP > View Discovered Community Names* to determine which addresses NetExplorer can discover.

If addresses show up with the name UNKNOWN, NetExplorer cannot access them. Determine what the community name for the unknown server is, and add that name to the Community List using *SNMP > Edit Community Name List*.

4. Use NXPCON to verify NetExplorer system status.

“Initial cycle completed” should be displayed in the NetExplorer System Status field. If the initial cycle is not complete, allow more time until it is completed.

Troubleshooting Your Windows Environment

If you experience problems with Windows, make sure your Windows environment accesses the files listed below and supplied with ManageWise 2.6. The ManageWise installation backs up any old versions of these files with an .OLD extension. These files are copied from the directory where CLNTCFG.EXE is executed (SYS:\LOGIN\MW\LDT by default).

CTL3D.DLL

I3DCTRLS.DLL

IDISPLAY.DLL

NWIPXSPX.DLL

NWNETAPI.DLL

WLS.DLL

VUSER.386

WUSER.EXE

Troubleshooting Your Btrieve Environment

This section provides solutions to problems you might encounter with Btrieve*.

How You Need to Load BSTART.NCF

Do not use the BSTART.NCF file as supplied with NetWare or manually load BTRIEVE.NLM and BSPXCOM.NLM with special parameters. Just load LDINV.NLM at the file server and allow it to load the Btrieve NLM files automatically. This loads the same defaults as those set when BTRIEVE.NLM and BSPXCOM.NLM are loaded without any special parameters.



Note If you have another application (for example, ARCserve*) that requires Btrieve, see "Problem: Conflicts between Btrieve and Other Applications."

Problem: LDISCAN.EXE Runs Out of Memory

If LDISCAN.EXE runs from a DOS prompt but seems to run out of memory during the login process, increase conventional memory or consider running LDISCAN.EXE outside of the login script. If your ManageWise Console workstation's Windows environment is low on memory (conventional or upper), you might see a MACHINES.DAT error. To free memory, unload some Windows applications or TSRs.

Problem: Conflicts between Btrieve and Other Applications

Inventory Manager might conflict with other programs based on the Btrieve database. If you experience problems, see your Btrieve manuals. Check to see that Btrieve is operating with at least the default values shown in the following table.



Note If you know the environment needs of your other application, add them to the ManageWise requirements and enter those values in BSETUP.NLM. If you are unsure, double the Btrieve defaults.

Parameter	Btrieve Defaults	Inventory Manager Requirements
Number of open files	20	3

Parameter	Btrieve Defaults	Inventory Manager Requirements
Number of handles (must be at least 3 times the number of sessions, below)	60	9
Number of locks	20	1
Number of transactions	0	0
Number of files per transaction	12	0
Largest compressed record size	0	0
Largest record size	8192	88
Largest page size	4096	4096
Number of sessions	15	3
Console refresh count	N/A	3
Create files as transactional	no	no
Logging of selected files	no	no

If another NLM file besides Inventory Manager requires Btrieve, use BSETUP.NLM to configure a BSTART.NCF file that loads BTRIEVE.NLM and BSPXCOM.NLM with enough file space for both applications.

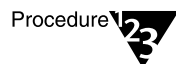
Problems with the Inventory Manager Database

If you are experiencing problems with your Inventory Manager database, or you changed Inventory Manager's Btrieve environment, you must rebuild the MACHINES.DAT, TYPES.DAT, FILES.DAT, and VALUES.DAT files in the SYS:\MW\LDT directory on the ManageWise Server.



These steps might be required if a power outage or other unexpected termination of the file server has corrupted the Btrieve files.

To rebuild the MACHINES.DAT, TYPES.DAT, FILES.DAT, and VALUES.DAT files



1. At the ManageWise Server console, enter

UNLOAD LDINV

and

UNLOAD LDISCAN

2. Enter

LOAD LDINV REMOVE

3. Enter

BSTOP

This unloads BSPXCOM.NLM and BTRIEVE.NLM.

4. At a workstation, delete the MACHINES.DAT, TYPES.DAT, FILES.DAT, and VALUES.DAT files in the administrator's network files directory (default SYS:\MW\LDT).

5. Delete or rename LDINV.ERR and any MACHINES.PRE, TYPES.PRE, FILES.PRE, and VALUES.PRE files.

6. In SYS:\SYSTEM, delete or rename BTRIEVE.TRN (if it exists).

7. To eradicate the deleted .DAT and .PRE files, enter

PURGE

8. At the ManageWise Server console, enter

LOAD LDINV FILE=SYS:\MW\LDT

9. At the ManageWise Server console, enter

LOAD LDISCAN INV_SERV=*servername* FILE=SYS:\MW\LDT

Substitute your path name as necessary.

10. At a workstation, enter

LDISCAN /V /S=*servername*

Alternatively, log in to the network. If you accepted the default Inventory Manager lines, LDISCAN.EXE runs in the System login script.

11. Restart the ManageWise Console workstation, and then enter

BREQUEST

BREQUEST.EXE can be loaded into high memory.

12. Load Inventory Manager from the ManageWise Control Panel in Windows.

Problem: Records Not Listed in the Inventory Manager Database

If the main Inventory Manager screen is empty after running <LDIScan Executable> /s=servername (the server specified under *Configure > Inventory Server*), copy the WBTRCALL.DLL and WBTRVRES.DLL files from the SYS:\PUBLIC directory to the administrator's ManageWise Desktop Management tools directory (C:\MW\LDT is the default). The inventory scanner executable <LDIScan executable> is LDISCAN.EXE for DOS, WLDISCAN.EXE for Windows 3.x, Windows 95, Windows 98, LDISCAN2.EXE for OS/2, and LDISCNNT.EXE for Windows NT.

Troubleshooting Desktop Management Problems

This section provides solutions to problems you might encounter with workstations managed by ManageWise.

Problem: You Get a Message about Loading SNMP VLM Files

Explanation	When you try to get information about workstations, you might get a message asking you to ensure that SNMP Virtual Loadable Module™ (VLM™) files were loaded.
Action	If this happens, you must configure the SNMP VLM files. Refer to <i>NetWare Client for DOS and MS Windows Users Guide</i> for this information.

Problem: Login Script Does Not Execute Properly

Explanation Configuration files must be installed on a workstation for you to be able to manage it from the ManageWise Console. The Client Configuration utility (CLNTCFG.EXE file) on the ManageWise Server executes automatically when a member of the MANAGEWISEGROUP user group logs in.

Action If the login script on a workstation does not execute properly, run CLNTCFG.EXE manually, as follows:

Procedure



1. **From Windows Program Manager, run CLNTCFG.EXE (located in SYS:MW\LDLT by default).**

Make sure any files CLNTCFG.EXE needs to copy to the workstations are located in the same directory as CLNTCFG.EXE. The files that CLNTCFG.EXE requires are listed in the file CLNTCFG.INI.

2. **If the workstation has been configured, a dialog box appears asking whether you want to reconfigure the workstation. Click Yes.**
3. **Click Configure.**
4. **Click Exit.**

Problem: You Cannot Control the Keyboard on a File Server with Desktop Management

Action Reload USER.NLM with the /OLDKB switch.

Resolving Time Discrepancies

NetWare 3.1x does not automatically adjust the time zone setting when daylight savings changes every six months.

The NetWare utility SYSTIME.EXE fixes some (but not all) time discrepancies between the ManageWise Server and workstations. Follow the instructions in the NetWare System Administration documentation under SET TIMEZONE.

Troubleshooting Your WAN Environment

Some WAN routers are set to filter SAP packets that certain Desktop Manager tools need to function properly. Inventory Manager requires routers to pass object type 0x0102 (OT_INTEL). Desktop Management requires routers to pass object type 0x0004 (the Novell OT_FILE_SERVER).

Technical Support and Update Information

How to Request Technical Support

To receive technical support, contact your local Novell reseller and request support.

For support on the NetWire electronic bulletin board, post questions in NOVMAN, section 2 (NetWare Mgmt. System). If you do not have a CompuServe* account, call CompuServe at 1-800-524-3388 or 1-614-457-0802 and ask for operator 200.

To place a call with Novell Technical Support, call 1-800-NETWARE (1-800-638-9273) or in the United States and Canada. All other locations, call 801-861-5588. If the issue is determined to be a software bug not previously reported, there is no charge for the support call.

How to Obtain Updates and Patch Files

The following section contains information on obtaining the latest available updates and patch files for products relating to ManageWise.

Virus Protection

You can download new virus signature files from the Cheyenne web site (<http://www.cheyenne.com>).



Note

We recommend that you download the most recent virus signature files regularly (at least once a month).

ManageWise

Updates and patches relating to ManageWise products are available on the web at the Novell® Technical Support site; point your browser at <http://www.novell.com/support/> and choose ManageWise from the “Choose a Product” list.

appendix **B** *Error Messages*

This appendix contains descriptions of error messages that you might receive while using ManageWise® and provides actions to take.

Agent Not Monitoring

Explanation This is a NetWare LANalyzer® Agent™ error.

Action Make sure the NetWare LANalyzer Agent NLM™ files (in LANZ.NCF) are running and check to see that the network board is being monitored from the server, as follows:

Procedure



1. **On the NetWare LANalyzer Agent server, load NWSNUT.**
2. **Load LANZCONF.**
3. **Select the network board driver that the message indicates is not being monitored, and then press Enter.**
4. **Select *Network Interface Items* from the menu.**
5. **Verify the following information:**
 - ◆ The Item column contains an entry labeled Statistics and the corresponding Status column indicates valid.
 - ◆ The Owner column indicates monitor.
 - ◆ The Network column indicates the name of the adapter.
6. **If all the information is correct, that interface should be monitored by NetWare LANalyzer Agent; skip to Step 7.**

If you have changed the network board in this server since the first time you installed NetWare LANalyzer Agent, it might take some time for NetExplorer™ software to record the new board in the database. If you do not want to wait for NetExplorer Manager to

update the database, you can update the MAC address of the network board manually by doing the following:

6a. In the ManageWise Console, click the server in a map.

6b. Select *Edit > Database Object*.

6c. Click the Adapter Information icon.

6d. Select the adapter that has changed.

6e. Click Edit.

—Change the MAC Address field to reflect the new node address on the server (type **config** at the server console to obtain this address).

—Enter a dummy value in the Make and Model field.

—Click OK.

7. If you have not changed the network board in this server since the first time you installed NetWare LANalyzer Agent, sometimes completing the following steps corrects the problem:

◆ Unload the NetWare LANalyzer Agent NLM files by typing **ULANZ** at the server console command prompt.

◆ Delete the **SYS:\LANZ\LANZ.CFG** file.

◆ Reload the NLM files by entering **LANZ** at the server console command prompt.

Btrieve 1002 or 2001 errors

Explanation These are Btrieve errors that indicate insufficient memory.

Action To free conventional memory, perform one or more of the following:

1. Close some of your open applications.
2. Unload any unnecessary TSRs.
3. Minimize your Windows program groups.

Btrieve 91 Error

Btrieve MACHINES.DAT, TYPES.DAT, FILES.DAT, and VALUES.DAT errors

Explanation These are Btrieve errors.

Action If you receive these messages, do the following:

- ◆ Verify that BREQUEST.EXE loads at the administrator workstation.
- ◆ Verify that you are using the same version of Btrieve on both the ManageWise Console and the ManageWise Server.
- ◆ Verify that you are using the correct version of Btrieve. Btrieve 6.10e is recommended.

This error can also occur if the MACHINES.DAT, TYPES.DAT, FILES.DAT or VALUES.DAT file becomes corrupted (for example, by a power outage). You might need to rebuild the inventory database and restore these .DAT files. For more information, see “Problems with the Inventory Manager Database” on page 98.

Communication with server failed (Error 251)

Explanation This is a NetWare Management Agent™ error that usually means the NETMAN user account on the server running NetWare Management Agent is corrupt.

Action Use the SYSCON or NWADMIN utilities to delete the account, re-create another user with the name NETMAN, and assign that user a password. (When using NWADMIN, make sure the context in which you create the NETMAN user is the same context as the ManageWise Server.)

Also, if you give the user a different password, remember to register that new password on the ManageWise Console.

Could not map ID of the user on the agent to a name.

Explanation This error occurs if the client workstations (Windows 98, Windows 95, Windows 3.x) are not logged into NDS.

Action On the client workstations, attach/login to the ManageWise server.

Error LANS001: Invalid temporary path

<\\servername\SYS\LOGIN\MW\LDT\SELTEMP\>

- | | |
|-------------|--|
| Explanation | This error can occur during login. A user might see this error when the desktop management TSR files are being loaded by a user who does not have the correct access rights to the SYS:\LOGIN\MW\LDT\SELTEMP directory on the ManageWise Server. |
| Action | Make sure that the user has Create, Read, Write, Erase, Modify, and FileScan rights on that directory. If the user is a member of the MANAGEWISEGROUP user group, verify that the MANAGEWISEGROUP user group has those rights on that directory. |

Instrumented OS Emulator unable to Register Object class: 100.3.1

- | | |
|-------------|---|
| Explanation | This is a NetWare Management Agent error. This message usually means a queue (such as a print queue) is corrupt. |
| Action | Try deleting the jobs in the queue. If this does not solve the problem, complete the following steps: <ol style="list-style-type: none">1. Delete the queue from the SYS:\SYSTEM directory.2. Run BINDFIX.3. Re-create the queue. |

ManageWise client Setup was unable to properly set the path for the Novell WUser Agent service. ManageWise client setup cannot complete successfully.

- | | |
|-------------|--|
| Explanation | This is an error message on Windows NT machines. On the Windows NT workstation/server, your user account should have administrator or administrator equivalent privileges. The Windows NT station configuration utility tries to add the Novell WUser Agent service, which is possible only if the user account has administrative privileges. |
| Action | When NTSTACFG.EXE is executed for the first time, the user who logs in should have appropriate administrator or administrator-equivalent permissions on the Windows NT machine. |

Module NETXPLOL.NLM not loaded retrying...

- | | |
|-------------|---|
| Explanation | This is a ManageWise Server error. It is sometimes displayed on the console of the ManageWise Server when the NetExplorer NLM files are |
|-------------|---|

loading. This is not a serious error; after the NLM files are all loaded, the message goes away and the software operates normally.

Action None.

No resources on probe

Explanation This is a NetWare LANalyzer Agent error. It can occur if

- ◆ SNMP is loaded with the incorrect parameters
- ◆ Another NLM is automatically loading SNMP without the parameters
- ◆ The upper limit on memory dynamically allocated by NetWare LANalyzer Agent was exceeded.

Action Perform the following actions:

- ◆ Make sure SNMP is loaded with the following parameters:

```
LOAD SNMP VERBOSE CONTROL= TRAP=
```

- ◆ If you have this statement in your AUTOEXEC.NCF file, make sure that another NLM is not automatically loading SNMP without the parameters.

To make sure that these parameters are being used, load CONLOG.NLM (point your browser at http://support.novell.com/search/ff_index.htm to get the Novell® File Finder utility and input the file name CONLOG.EXE) to review the loading of the NLM files. When SNMP loads, it should return the following message:

```
SNMP: ControlCommunity now accepts any community name
```

- ◆ If it seems that the upper limit on memory that can be allocated dynamically by NetWare LANalyzer Agent has been exceeded, refer to the bound= parameter in the SYS:\SYSTEM\LANZ.NCF file for an explanation on increasing or decreasing the memory used by NetWare LANalyzer Agent.

No Response

Explanation This is a NetWare LANalyzer Agent error.

Action Complete the following steps:

1. Make sure the network segment is pointing to an active remote monitor by doing the following:
 - a. In a ManageWise Console window, select the segment reporting no response.

You can select a segment from the View > All > Network Segments window or the Internetwork map.
 - b. Select the *Edit > Database Object* command
 - c. Scroll down to the NetWare LANalyzer Server icon and select it.
 - d. Select an active LANalyzer server.
 - e. Click Save.
2. Select the *Fault > Test Connectivity* command to verify that the ManageWise Console can communicate with the server running NetWare LANalyzer Agent; perhaps an intermediate device is down.

Out of Top N resources

Explanation This is a NetWare LANalyzer Agent error.

Action Complete the following steps:

1. Make sure SNMP is loaded with the following parameters:

```
LOAD SNMP VERBOSE CONTROL= TRAP=
```

If you have this statement in your AUTOEXEC.NCF file, make sure that another NLM is not automatically loading SNMP without the parameters. To make sure that these parameters are being used, load CONLOG.NLM (point your browser at http://support.novell.com/search/ff_index.htm to get the Novell® File Finder Web utility and input the file name CONLOG.EXE) to review the loading of the NLM files. When SNMP loads, it should return the following message:

SNMP: ControlCommunity now accepts any
community name

If the error message is still reported, continue to Step 2.

2. Take one of the following actions:

- a. In the ManageWise Console, close any Network Dashboard™ window or Top 20 Station Table window that you are not using.
- b. On the NetWare LANalyzer Agent Server, increase the Top N resources value in the SYS:\SYSTEM\LANZ.NCF file. This file contains a detailed description of the Top N resources variable.
- c. You can also use the LANZCONF utility on the NetWare LANalyzer Agent Server to see how many Top N tables have been opened by completing the following steps:
 - Load NWSNUT.
 - Load LANZCONF.
 - Select the network board driver that is being monitored.
 - Select *Network Interface Items* from the menu.
 - Count how many Host Top N entries are in use.

Each entry shows which console and service (Network Dashboard or Station Table) owns it.

Unable to access default security parameters

Explanation	This is a Desktop Management error.
Action	Edit the default Access Rights List by following the procedure shown in <i>ManageWise 2.6 Desktop Management Guide</i> .

Unable to read user's Access Rights List on server

Explanation	This is a Desktop Management error.
Action	Edit the default Access Rights List by following the procedure shown in <i>ManageWise 2.6 Desktop Management Guide</i> .

User Agent connected to the DS <Server Name>. Connect to the <Server Name> to get the security information.

Unable to access security information.

Unable to connect to user's Novell Directory Services tree.

Explanation These are Desktop Management errors. This problem is manifested by an inability to access security information and an inability to connect to user's Novell Directory Services tree. The ManageWise Console is unable to connect to the server from which the client (user agent) workstation derived its security template. The Console is not able to access the security template information for the user agent.

Action On the ManageWise Console, attach or login to the server to which the client workstation is connected to.

Wrong version of DLL CTL3D.DLL

Explanation This message is usually the result of low memory, but can also occur if you are using an incorrect version of the CTL3D.DLL file.

Action Free more conventional memory.

If you need to install the correct version of the CTL3D.DLL file, follow these steps:

Procedure



- 1. Change directories to your Windows SYSTEM directory.**
- 2. Back up CTL3D.DLL.**
- 3. Copy SYS:\LOGIN\MW\LD\CTL3D.DLL to \WINDOWS\SYSTEM.**

You have no console privileges on this server

Explanation This is a Desktop Management error. This message can mean that you are attempting to perform a task directed at a server to which you are not currently attached.

This message can also mean that you do not have sufficient rights to perform the task. Console privileges are available to users who are SUPERVISOR-equivalent or who were granted console operator rights. Use SYSCON or NWADMIN to verify or modify the user rights.

Action Ensure that you are attached to the target server and that you have appropriate console privileges to perform the task.

appendix **C** *ManageWise Server Backups*

This appendix provides information about backing up various files on servers.

Server Backups and NetWare LANalyzer Agent Files

When you back up the server on which NetWare® LANalyzer® Agent™ software is loaded, *do not* back up SYS:\LANZ\LANZ.CFG.

Warning



NetWare LANalyzer Agent uses this file during its operation. Backing up open files can cause the backup to fail.

Server Backups and NetExplorer Files

When you back up the server on which NetExplorer™ software is installed, *do not* back up the following files and directories:

SYS:\NMDISK\NETXPLOR.DAT

SYS:\NMDISK\NXPIPX.INI

SYS:\NMDISK\NXPIP.INI (if it exists)

SYS:\NMDISK\NXP.INI

SYS:\NMDISK\NLA.ADR

SYS:\NMDISK\DATSAV (directory)

SYS:\NMDISK\NXPWORK (directory)

Community string file for NXPIP (if you created one)

Community string file for NXPLANZ (if you created one)

Warning



NetExplorer uses these files during its operation. Backing up open files can cause the backup to fail.

appendix **D** ***Changes Install Makes to the ManageWise Server***

This appendix describes the changes that network management software, NetWare® LANalyzer® Agent™ software, NetWare Management Agent™ software, and Desktop Manager makes to the ManageWise® Server. It also provides information about some utilities and parameters that you can use to change the default behaviors.

Refer to the InocuLAN AntiVirus for NetWare Supervisor's Guide for information about anti-virus software.

This appendix is divided into the following sections:

- ◆ "Server Installation Notes for Network Management"
- ◆ "Server Installation Notes for Desktop Management"
- ◆ "Bindery Objects Created by ManageWise"

Server Installation Notes for Network Management

This section describes the changes that the ManageWise installation program makes to your server for network management.

Overview of Network Management Installation on the ManageWise Server

When you install ManageWise on a server, the installation program does the following:

- ◆ Copies files to the SYS:\NMDISK directory, the SYS:\MW directory, the SYS:\LANZ directory, and the SYS:\SYSTEM directory.
- ◆ Creates backup files that are stored in directories (SYS:\SYSLZNLM.SAV, for example).
- ◆ Modifies the SYS:\SYSTEM\AUTOEXEC.NCF file to load NLM™ files required by ManageWise and the management agents.
- ◆ Prepares the following files in the SYS:\SYSTEM directory:
 - ◆ LANZ.NCF
 - ◆ NETXPLOE.NCF
 - ◆ NMA2.NCF
 - ◆ NMA5.NCF (NetWare 5 only)
 - ◆ NMSBASE.NCF

The installation program backs up all the system files it updates to enable you to undo the installation changes, if necessary. The backed up files are placed in .SAV directories on the SYS: volume.

Modifications to the AUTOEXEC.NCF File

ManageWise installation adds lines to the AUTOEXEC.NCF file. These lines include comments and instructions for removing comment marks (#) from the file.

Installation of the LANZ.NCF File

ManageWise installation puts the LANZ.NCF file in the SYS:\SYSTEM directory and adds a line that executes the file to the target server's AUTOEXEC.NCF file. The LANZ.NCF file contains all the NetWare system LOAD commands required for NetWare LANalyzer Agent software.

Installation of the NETXPLOD.NCF File

The NETXPLOD.NCF file loads the discovery NLM files and describes the order in which the files are loaded. The NETXPLOD.NCF file also provides command options suitable for various network configurations.

Installation of the NMA2.NCF File

ManageWise installation puts the NMA2.NCF file in the SYS:\SYSTEM directory and adds a line that executes the file from the target server's AUTOEXEC.NCF file. The NMA2.NCF file loads the NLM files required for the NetWare Management Agent software to run on NetWare 3.1x and NetWare 4.x servers.

Installation of the NMA5.NCF File

ManageWise installation puts the NMA5.NCF file in the SYS:\SYSTEM directory and adds a line that executes the file from the target server's AUTOEXEC.NCF file. The NMA5.NCF file loads the NLM files required for the NetWare Management Agent software to run on NetWare 5 servers.

Installation of the NMSBASE.NCF File

ManageWise installation puts the NMSBASE.NCF file in the SYS:\SYSTEM directory and adds a line that executes the file from the target server's AUTOEXEC.NCF file. The NMSBASE.NCF file loads the NLM files required prior to loading the NetExplorer™ software, NetWare Management Agent software, and NetWare LANalyzer Agent software.

Server Installation Notes for Desktop Management

This section describes the changes that the ManageWise installation makes to your server for workstation management.

Overview of Desktop Management Installation on the ManageWise Server

ManageWise installation might ask you to confirm changes to the target server's AUTOEXEC.NCF file and login script, depending on where you target your installation. At the time you confirm these changes, you can view and edit the modifications you are asked to accept.

The installation places a command in the target server's AUTOEXEC.NCF file that calls the MW_AUTO.NCF file. This file consists of commands to load the NLM files required by ManageWise.

The ManageWise installation might also place a command into the appropriate login script. If you target a NetWare 3.1x server, the installation asks to modify the system login script for that server. If you target an NDS tree and organizational unit (OU), the installation asks to modify the system login script for that OU.

The ManageWise Login script consists of commands to scan users' workstations for hardware and software inventory data and to load the User agents required by ManageWise Desktop Manager.

Modifications to the AUTOEXEC.NCF File

The ManageWise installation places a command in the target server's AUTOEXEC.NCF file that calls the MW_AUTO.NCF file. This file consists of commands to load NLM files required by ManageWise. Before you can use ManageWise, you must load the appropriate NLM files.

The following lines are added to the ManageWise server's AUTOEXEC.NCF file:

```
REM *** BEGIN Desktop Management Section ***
    MW_AUTO.NCF
REM *** END Desktop Management Section ***
```

The ManageWise installation makes a backup of your current AUTOEXEC.NCF file before making these changes. The backup is named AUTOEXEC.00x.

The MW_AUTO.NCF file might consist of the following:

```
REM The following commands load the NLMs
    required
REM by Desktop Manager.
LOAD USER
LOAD LDINV.NLM FILE=<SYS:MW\LDT>
LOAD LDISCAN INV_SERV=<SERVERNAME> FILE=<SYS:MW\LDT> SCANNOW
```

NetWare Login Script Changes to Support User Management

The ManageWise installation places commands into the appropriate login script affecting client workstations that are members of the MANAGEWISEGROUP user group at login.

The login script consists of the following:

```
REM *** BEGIN ManageWise Desktop Management Section ***
IF MEMBER OF ".MANAGEWISEGROUP.<context>" THEN
MAP ERRORS OFF
MAP ins S1:=L:
MAP L:=<ManageWiseServerName>\SYS:
INCLUDE L:\PUBLIC\MW_LOGIN.DAT
MAP L:=S1:
MAP del S1:
MAP ERRORS ON
END
REM *** END ManageWise Desktop Management Section ***
REM ***** BEGIN ManageWise INOCULAN Virus Protect Section
IF MEMBER OF ".MANAGEWISEGROUP.<context>" THEN
IF <OS> = "WINDOWS_NT" THEN
REM **NT WORKSTATION ** NOTHING TO DO
ELSE
MAP L:=<ManageWiseServerName>/SYS:
#L:\INOCULAN\AVUPDATE.EXE /Q
END
END
REM ***** END ManageWise INOCULAN Virus Protect Section
```

When you install to an OU, the installation finds the login script attribute of the OU and backs it up to a file named NET\$LOG.00x.

When you install to a bindery server, the installation makes a backup of your current login script. The backup is named NET\$LOG.00x.

If you have not installed ManageWise before, or if you have installed previous versions of ManageWise and placed the ManageWise section after an EXIT statement, be aware that the installation adds the new ManageWise section to the end of your login script.

The ManageWise Login script contains commands to install the ManageWise user management agents, if they are not installed already. It then runs the inventory scan program.

The MW_LOGIN.DAT file section consists of the following:

```
REM === ManageWise Desktop Management Include file for System Login ===
IF <OS> = "WINDOWS_NT" THEN
#\\<ManageWiseServerName>\SYS\MW\LDT\ntstacfg /ipx /
L=\\<ManageWiseServerName>\SYS\MW\LDT\SELTEMP /NOUI
#\\<ManageWiseServerName>\SYS\MW\LDT\LDISCNNT /S="<ManageWiseServerName>"
/V /i=\\<ManageWiseServerName>\SYS\MW\LDT\ldappl.ini
ELSE
IF "%<WINBOOTDIR>" = " " THEN
#L:\MW\LDT\OSVER
IF ERROR_LEVEL = "1" THEN
#L:\MW\LDT\LDISCAN /S=<ManageWiseServerName>
#L:\MW\LDT\DOSCFG /L=\\<ManageWiseServerName>\SYS\MW\LDT\SELTEMP /
S=\\<ManageWiseServerName>\SYS\MW\LDT
ELSE
#L:\MW\LDT\CLNTCFG
#L:\MW\LDT\WLDISCAN /S=<ManageWiseServerName>
END
ELSE
#L:\MW\LDT\CLNTCFG
#L:\MW\LDT\WLDISCAN /S=<ManageWiseServerName>
END
END

REM === End Include File ===
```

Support for Temporary Drive Mapping

The following lines in the ManageWise Login script describe how the temporary drive mappings are stored when loading ManageWise user agents on Windows 3.x, Windows 95, Windows 98, and DOS workstations.

```

REM *** BEGIN ManageWise Desktop Management Section ***
IF MEMBER OF "MANAGEWISEGROUP" THEN
IF <OS> = "WINDOWS_NT" THEN
INCLUDE \\<SERVERNAME>\SYS\PUBLIC\MW_LOGIN.DAT
ELSE
MAP ERRORS OFF
MAP S1:=L:
MAP L:=<SERVERNAME>
INCLUDE L:\PUBLIC\MW_LOGIN.DAT
MAP S1:=L:
MAP ERRORS ON
END
REM *** END ManageWise Desktop Management Section ***

```

The existing drive mappings are stored and retrieved. This enables the installation to include the Scan programs and client configuration commands in the ManageWise Login script. On saving the current drive mapping for L:, it is temporarily mapped to the shared MANAGEWISE directory (SYS:\MW\LDT, by default). Before MW_LOGIN.DAT returns to the login script, the saved drive mapping is retrieved.

Inventory Scan Programs

The scan programs perform an inventory scan of local hardware and software at each login for use with Desktop Manager.

Desktop Manager uses four platform-dependent scan programs to discover hardware and software information on client workstations.

Table 4-1
Scan Programs

Program	Platform and Protocol
LDISCAN.EXE	DOS
WLDISCAN.EXE	Windows 3.x, Windows 95, Windows 98 over IP and IPX
LDISCNNT.EXE	Windows NT server and workstations over IPX
LDISCAN2.EXE	OS/2 over IPX
Inventory MacScan	Macintosh

The following lines in the Login script describe and run the Scan Programs on the workstations.

For DOS workstations,

```
#L:\MW\LDL\LDISCAN /S=<SERVERNAME>
```

For Windows 3.x, Windows 95, Windows 98 workstations

```
#L:\MW\LDL\WLDISCAN /S=<SERVERNAME>
```

For Windows NT workstations,

```
#\\<SERVERNAME>\SYS\MW \LDL\LDISCNNT /<IP/IPX>  
/S="<SERVERNAME>" /V  
/I=\\<SERVERNAME>\SYS\MW\LDL\LDAPPL.INI
```

Refer to *ManageWise 2.6 Desktop Management Guide* for more information on the Inventory Scan programs.

Loading and Configuring User Agents on DOS Workstations

USERTSR.EXE and POPUPTSR.EXE are two TSRs needed to remotely control and obtain diagnostic information from a full-screen DOS workstation in graphics mode. To provide continual access to these workstations, the TSRs should always be loaded. Together, USERTSR.EXE and POPUPTSR.EXE need 12 KB of memory.

USERTSR.EXE accepts the following command-line options.

```
USERTSR [?] [REMOVE] [NOMOUSE] [OLDEGA] [SNOW]  
[LOADHIGH] [STEALTH] [PERMISSION] [FIXED]
```

Option	Description
?	Displays the help message for USERTSR.EXE.
REMOVE	Unloads USERTSR.EXE from memory.
NOMOUSE	Disables mouse control. Viewers cannot control a mouse when this option is used.

Option	Description
OLDEGA	Installs USERTSR.EXE for old-style EGA adapters that do not have readable registers (especially older Paradise adapters). Use this option only if you are having trouble controlling an EGA-based station.
SNOW	Reduces "snow" that might appear on the screen when controlling a station running in CGA text mode.
LOADHIGH	Moves the resident portion of USERTSR.EXE to upper DOS memory.
STEALTH	Loads USERTSR.EXE without displaying the blue copyright banner.
PERMISSION	Forces user permission. A workstation cannot be viewed until permission is given.
FIXED	Forces USERTSR.EXE to be nonremovable.

POPUPTS.R.EXE accepts the following command-line options.

```
POPUPTS.R [/L=path] [/T=path] [/H=hotkey] [/R] [/M]
          [/S] [/E]
```

Option	Description
/L=< <i>path</i> >	Shows the full pathname of the directory where the LANMENU.DAT file is stored. A default LANMENU.DAT file is in the shared MWCLIENT subdirectory on the Client workstation.
/T=< <i>path</i> >	Shows the full pathname of the directory in which POPUPTS.R stores temporary files.
/H=< <i>hotkey</i> >	Overrides the default hot key combination used to call up POPUPTS.R.

Option	Description
/R	Removes POPUPTSR from workstation memory.
/M	Disables the use of expanded memory at the workstation.
/S	Shows the current status of POPUPTSR.
/E	Displays the last error POPUPTSR encountered.

Bindery Objects Created by ManageWise

ManageWise creates four objects in the bindery or in NDS. On NetWare 3.x™ servers, only the MANAGEWISEGROUP user group is visible (through SYSCON). On NetWare 4.1x and NetWare 5 servers using bindery emulation, three other objects are visible in NDS using the NetWare Administrator utility. These other objects are as follows:

- ◆ Novbind5+258
- ◆ Intel Asset Manager+258
- ◆ Lansight Security Template+258

The Novbind5+258 object is created in the bindery context that was listed first when ManageWise was run. The Intel Asset Manager+258 and Lansight Security Template+258 objects are created in the OU where the ManageWise Server resides.

Warning



Do not delete these objects. Deleting these objects can interfere with the proper operation of ManageWise.

- ◆ If you delete the Novbind5+258 object, you must reinstall ManageWise on the server to re-create the object.
- ◆ If you delete the Intel Asset Manager+258 object, you can re-create it by unloading and reloading LDINV.NLM (with the parameters specified in the AUTOEXEC.NCF file) on the ManageWise Server.

- ◆ If you delete the Lansight Security Template+258 object, you can re-create it by performing the steps regarding creation of the security templates.



You can delete the MANAGEWISEGROUP user group if you created another group to replace it or are using Profile objects to control which users are managed with the ManageWise software.

appendix **E** ***Install Changes to the ManageWise Console and Workstations***

By default, the ManageWise® installation makes changes to the SYSTEM.INI, and WIN.INI files on the workstation you designate as the ManageWise Console. This appendix describes these changes.

Changes to the SYSTEM.INI File

Changes to the [386Enh] section of the SYSTEM.INI file on the ManageWise Console and workstations load necessary Windows drivers. The following lines are added to the [386Enh] section of the SYSTEM.INI file:

```
device=VUSER.386  
TimerCriticalSection=10000
```

The ManageWise installation makes a backup of your current SYSTEM.INI file before making this change. You can find the backup of SYSTEM.INI in MW\BACKUP.

Changes to the WIN.INI File

The ManageWise installation program makes changes to the ManageWise Console and workstation's WIN.INI file by default. The following lines are added:

ManageWise Console

```
[Windows]  
load=nmscron.exe  
[ddeml]  
ShutdownTimeout=10000
```

Workstation

```
[Windows]  
load=wuser.exe
```

The ManageWise installation makes a backup of your current WIN.INI file before making this change. You can find the backup of WIN.INI in MW\BACKUP on the ManageWise Console or the WINDOWS directory on the workstation.

appendix **F** ***Changes Desktop Remote Makes to Your Workstation***

The Desktop Remote installation process makes the following changes to your Windows 3.x, Windows 95, Windows 98 and Windows NT system:

- ◆ Copies VUSER.386 to your Windows SYSTEM directory.
- ◆ Adds the following line to the [386Enh] section of your SYSTEM.INI file.

```
device=VUSER.386
```

- ◆ Creates a directory for Desktop Remote and installs the following Desktop Remote files to that directory.

File	Purpose
DTMODEM.CFG	Contains the modem database.
DTREMOTE.CFG	Contains the phone book, security settings, and other encrypted information.
CTL3D.DLL	Contains interface functionality used by DTREMOTE.EXE.
DTREM.DLL	Contains application functionality used by DTREMOTE.EXE.
DTREMOTE.EXE	Desktop Remote program executable.
WASYNC.EXE	Contains the Viewer window functionality used by DTREMOTE.EXE.
AARB.DLL	Monitors incoming calls on the selected COM ports and routes them to the service requested.
COEXIST.DLL	Allows the workstation to be controlled over the network and over a modem at the same time.

appendix **G** ***NetExplorer Theory of Operations***

ManageWise® software discovers network topology and displays that topology on the ManageWise maps. NetExplorer™ software drives the ManageWise discovery process. NetExplorer discovers network systems and places them in the ManageWise database. The ManageWise network maps are then created from information stored in this database.

This appendix describes the components of NetExplorer, provides a detailed theory of operation, and discusses the categories of network systems that NetExplorer discovers.

NetExplorer System Components

The NetExplorer system consists of these interdependent components:

- ◆ NetExplorer Manager, on the ManageWise Console—updates the ManageWise database with data collected by the NetExplorer components on the NetExplorer Server.
- ◆ NETXPLOL.NLM, on the NetExplorer Server—communicates with NetExplorer Manager and with the discovery NLM™ files (NXPIPX.NLM, NXPIP.NLM, and NXPLANZ.NLM) that are actively discovering network objects; stores data in the sequential NETXPLOL.DAT file.
- ◆ NXPIPX.NLM, on the NetExplorer Server—discovers various NetWare® systems on IPX™ networks and NetWare/IP™ networks; sends information about systems to NetExplorer.
- ◆ NXPIP.NLM, on the NetExplorer Server—discovers IP routers on IP networks; sends information about routers to NetExplorer.
- ◆ NXPLANZ.NLM, on the NetExplorer Server—communicates with NetWare LANalyzer® Agent™ software and LANtern™ network

monitors to gather information about all systems communicating on the segments they monitor; sends information about systems to NetExplorer.

- ◆ NXPCON.NLM, on the NetExplorer Server—used to configure the discovery system and view discovery status information.
- ◆ MEMMGR.NLM, on the NetExplorer Server—general-purpose memory manager, which all NetExplorer NLM files call.

NetExplorer modules discover and store information in the NETXPLO.DAT file in your SYS:\NMDISK directory.

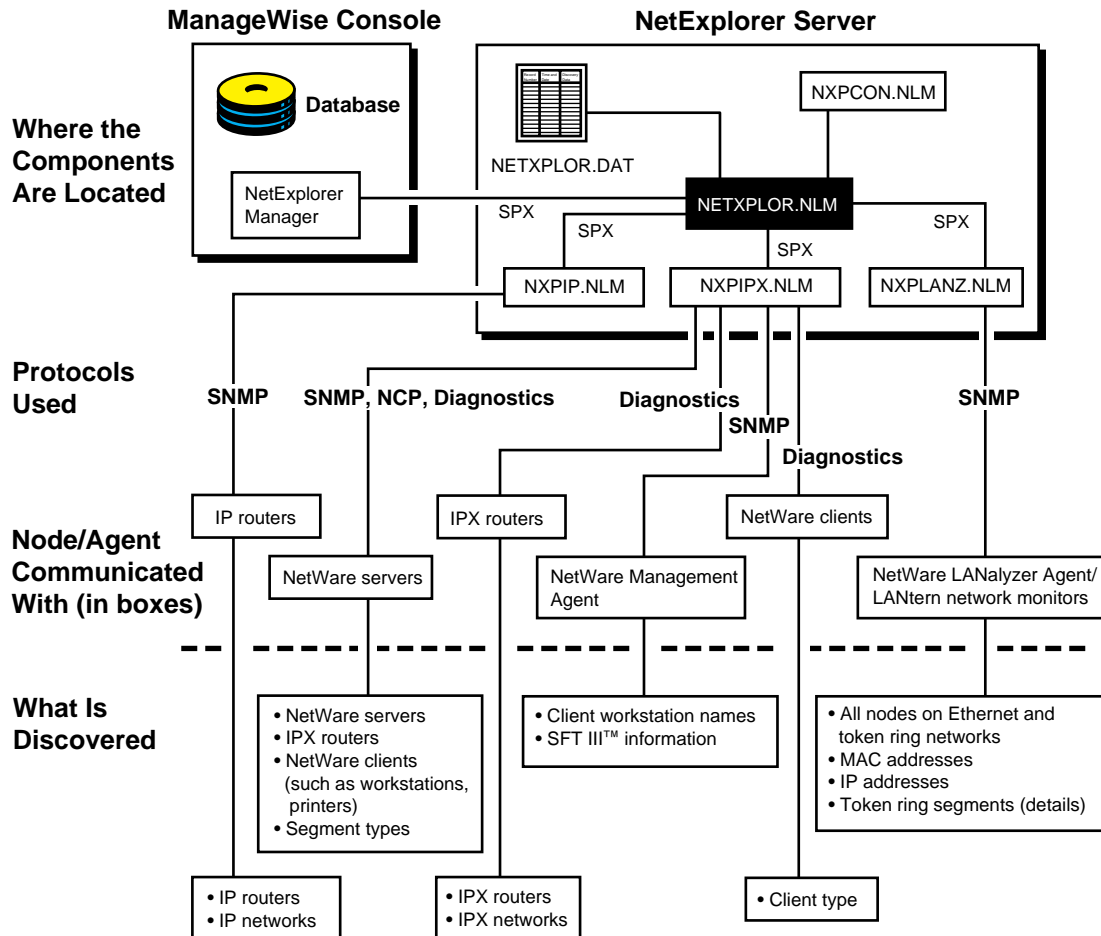
Figure G-1 illustrates the architecture of the NetExplorer discovery system and shows the roles of the various components, network systems, and agent software.

Note



NetExplorer uses NetWare Management Agent™ software, NetWare LANalyzer Agent software, and LANtern network monitors to obtain certain discovery information. Using these agents throughout your network enhances the accuracy and detail of logical maps displayed by the ManageWise Console; however, they are not required.

Figure G-1
NetExplorer Discovery System Architecture



NetExplorer Manager Software

NetExplorer Manager resides on the ManageWise Console along with the ManageWise database. NetExplorer Manager retrieves discovery data from the NetExplorer Server, schedules and starts NetExplorer updates to the ManageWise database, and generates discovery alarms. Each ManageWise Console maintains its own separate database. A single NetExplorer Server can support several ManageWise Consoles at any given time.

NetExplorer NLM Software

The NetExplorer NLM software resides on the NetExplorer Server. It consists of NETXPLOE.NLM, NXPCON.NLM (a utility to configure and monitor NetExplorer operation), and the discovery NLM software.

After the discovery NLM software obtains information about these systems, it is communicated to NETXPLOE.NLM, which saves it in a local file (NETXPLOE.DAT) and forwards this information to NetExplorer Manager on the ManageWise Console. “NetExplorer NLM Processes” describes the NetExplorer NLM processes, which query the network for different sets of systems.

Representation of Systems in the ManageWise Logical Maps

If a system has more than one of the services listed in Table G-3, ManageWise picks an icon to represent it, based on one of its services. You can change this icon using the database object editor.

If a system has either an IPX or IP router service, ManageWise considers it a router and shows it on the internetwork map, as well as on the segment maps.

SAP IDs

SAP (Service Advertising Protocol) filtering prevents routers from passing SAP packets. However, ManageWise Consoles, HMI™ hubs, NetWare Management Agent, NetWare LANalyzer Agent, and the NetExplorer NLM software use SAP to identify themselves to other ManageWise components. As a result of SAP filtering, alarms sent by NetWare Management Agent do not reach the ManageWise Console, and the ManageWise Console cannot identify all the manageable servers and HMI hubs.

To enable the NetExplorer Server and ManageWise Console to receive the SAP packets that identify manageable servers, HMI hubs, and other servers, configure the router that is filtering SAP packets to list the specific SAP numbers that it should pass.

NetWare systems and ManageWise components use the SAP numbers listed in Table G-1.

Table G-1
SAP ID Table

Component	SAP Number (Decimal)	SAP Number (Hexadecimal)
ManageWise Console	618	26A
NetExplorer NLM	567	237
NetWare Management Agent 2.6	635	27B
ManageWise Agent™ for Windows NT Server	651	28B
Virus Protect	258	102
HMI hub	569	239
NetWare LANalyzer Agent	570	23A
Print server	7	7
Advertising print server	71	47
NetWare file server	4	4

NetExplorer NLM Processes

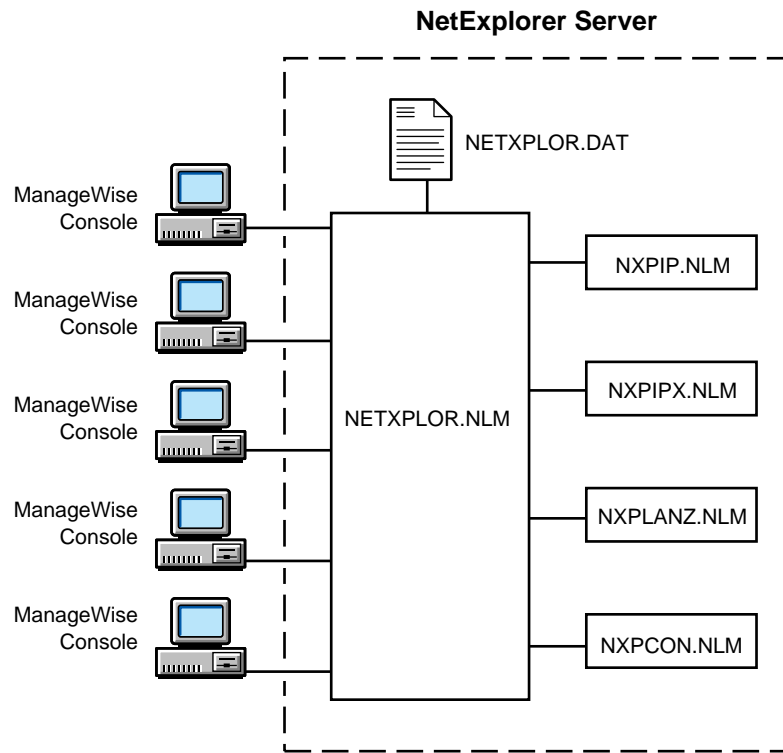
As described in the sections that follow, each of the following three NetExplorer NLM processes queries the network using different methods to discover systems:

- ◆ NXPIP.NLM
- ◆ NXPIPX.NLM
- ◆ NXPLANZ.NLM

These NLM processes communicate through NETXPLO.NLM to the ManageWise Console. Figure G-2 shows the relationship of the discovery NLM processes, NetExplorer, and the ManageWise Console. “NetExplorer Discovery Process” on page 139 describes how these

pieces operate together to discover the contents and topology of a network.

Figure G-2
NetExplorer NLM
Software



NXPIP.NLM

NXPIP.NLM is installed on the NetExplorer Server. It uses SNMP to discover IP routers. You should enable NXPIP.NLM only if you have IP routers on your network. To use this NLM, your NetExplorer Server must also be running TCP/IP, and TCP/IP must be bound to at least one of your network's interface boards. NXPIP.NLM uses MIB-II information, such as the system table, routing table, interface table, interface data-link type and frame type, and segment data-link type. Note that because there are different versions of implementation of MIB-II for different vendors, the information you receive might differ, depending on which vendor you use.

NXPIPX.NLM

NXPIPX.NLM is installed on the NetExplorer Server. It uses a variety of NetWare, SNMP, and IPX protocols, such as IPX diagnostics, to discover NetWare servers, IPX routers, and IPX workstations.



Note

You should never disable NXPIPX.NLM.

NXPLANZ.NLM

NXPLANZ.NLM is installed on the NetExplorer Server. It queries NetWare LANalyzer Agent software and LANtern network monitors for information about all the systems that exist on their network segments, regardless of protocol.

You should always enable NXPLANZ.NLM if you have NetWare LANalyzer Agent software or LANtern network monitors on a network segment.

In the case of source-routed token ring networks, make sure that you have NetWare LANalyzer Agent software running on every token ring in your network to discover your network topology correctly.

Additional ManageWise Components in a ManageWise Network

NXPIP.NLM, NXPIPX.NLM, and NXPLANZ.NLM operate in conjunction with the following network components:

- ◆ NetWare LANalyzer Agent servers
- ◆ NetWare Management Agent servers
- ◆ NetWare servers

NetWare LANalyzer Agent Servers

NetWare LANalyzer Agent is a set of NLM files that provides network analysis of Ethernet, token ring, or FDDI segments. NetWare LANalyzer Agent discovers all systems on the segments it monitors, regardless of the protocols the systems use. You can monitor multiple segments by putting agents on each segment or by using the multisegment version of the software on a server connected to multiple

segments. The NXPLANZ.NLM software on the NetExplorer Server queries NetWare LANalyzer Agent servers using SNMP for information about each of the systems that resides on their segments. NetWare LANalyzer Agent is available separately and can be installed on any NetWare 3.x, NetWare 4.x, or NetWare 5 server. NetWare LANalyzer Agent comes with a one-user version of NetWare so that it can also be installed on a dedicated machine.



We highly recommend that you have NetWare LANalyzer Agent monitoring each source-routed token ring segment for the discovery process to be most effective.

Like the NetWare LANalyzer Agent software, LANtern network monitors discover all systems on the network segment they are installed on. This information is then made available to queries from NXPLANZ.NLM. A LANtern network monitor operates on a single Ethernet segment and communicates only using the IP protocols. Like NetWare LANalyzer Agent, it recognizes all systems, regardless of protocol.



By default, NetWare LANalyzer Agent continues to report systems for seven days after they are discovered. If you decrease this timer to one day, you will detect devices that move from one segment to another faster.

NetWare Management Agent Servers

NetWare Management Agent servers are any NetWare 3.11, NetWare 3.12, NetWare 4, or later servers with NetWare Management Agent installed. NetWare Management Agent 2.6 servers respond to SNMP queries from NXPIPX.NLM with the username and address of those workstations that are logged in to the server. NXPIPX.NLM obtains SFT III server information from NetWare Management Agent 2.6. For best results, we recommend that you install NetWare Management Agent 2.6 on every NetWare 3TM, NetWare 4, or NetWare 5 server on your network.

NetWare Servers

NXPIPX.NLM queries all NetWare servers for information in their tables. All NetWare servers allow their binderies to be examined by the discovery process when their security settings are set to default values.



For the NetExplorer NLM software to discover login names of workstations attached to a NetWare server, NetWare Management Agent 2.6 must be installed on the server.

NetExplorer Discovery Process

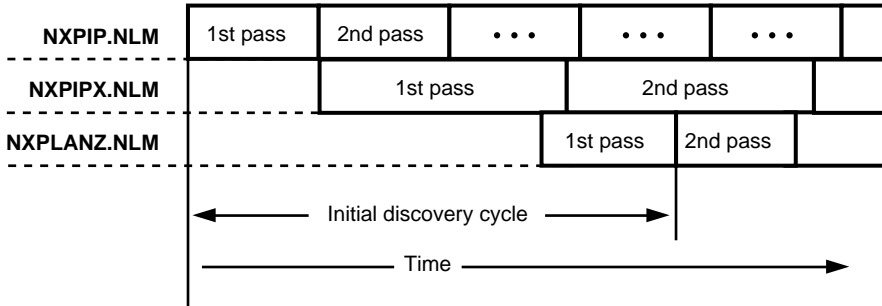
You can configure NetExplorer to discover your network continually or to discover your network according to a schedule you specify. The following sections discuss the discovery process.

Continuous Discovery

NetExplorer discovery discovers the internetwork that it resides on through a process initiated and controlled by NETXPLOE.NLM. Initially, each discovery NLM identifies itself to NETXPLOE.NLM. NETXPLOE.NLM then begins the initial discovery cycle starting with NXPIP discovery, followed by NXPIPX discovery, and finally NXPLANZ discovery. Information gathered by NetExplorer is stored in the NETXPLOE.DAT file on the NetExplorer Server.

Figure G-3 shows each of the discovery processes in relationship to time. As shown, after NXPIP finishes its first pass, NXPIPX begins, and NXPIP starts over again. After NXPIPX finishes its first pass, NXPLANZ begins and NXPIPX starts its second pass. All three of the discovery processes run continually to detect changes to the network, unless otherwise directed. Any changes to the network are saved as records in the NETXPLOE.DAT file. When all three discovery processes have completed one pass, the initial discovery cycle is complete.

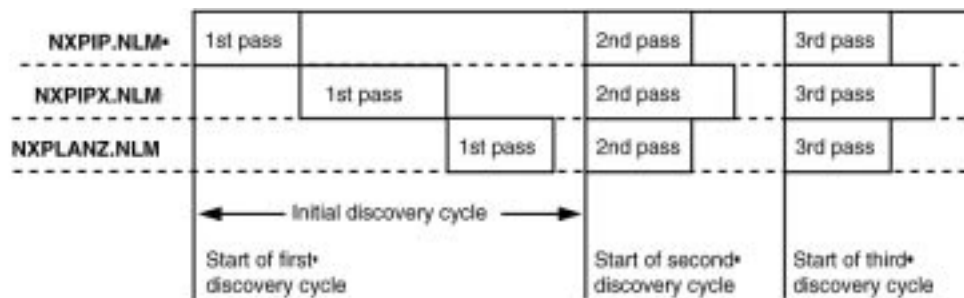
Figure G-3
Discovery Cycle Timing Sequence—
Continuous Discovery Mode



Scheduled Discovery

Scheduled discovery works similarly to continuous discovery except that the discovery processes are only allowed to run during certain time periods each week. You can set the schedule using the NXPCON utility on the NetExplorer Server. Schedule intervals are specified by a start time and a duration. It is important that you set your schedule time to be greater than or equal to one cycle time, to attain complete discovery. When the end of the scheduled interval is reached, discovery operations are suspended. Discovery resumes at the start of the next scheduled interval. In addition, if discovery is limited to one pass during an interval, each discovery process is suspended if it reaches the end of a pass before the interval has expired. This is shown in Figure G-4.

Figure G-4
Discovery Cycle Timing Sequence—
Scheduled Discovery Mode



NXPIP

The first sequence in the NetExplorer discovery cycle involves the discovery of IP routers. NXPIP locates its local router using TCP/IP configuration information and queries it for the identity of other routers on the network. It then queries the MIBs on the routers using SNMP. The following information is then collected: IP addresses, interface types, and MAC addresses.

You define the scope of NXPIP discovery. By default, the IP scope is the IP network of any IP networks to which the NetExplorer Server is connected, as defined by the class of the network. For example, if the

NetExplorer Server's IP address is 10.59.6.22, the IP discovery NLM discovers the entire 10.59.0.0 network and its subnets. You can restrict or expand the scope by specifying scoping information using NXPCON.

NXPIPX

After NXPIP completes its first pass, NXPIPX begins discovery. Discovery begins at the NetExplorer Server. NXPIPX uses a series of techniques, including SNMP, RIP, and IPX and SPX™ (Sequenced Packet Exchange™) diagnostics to discover the attached IPX or NetWare/IP internetwork. NXPIPX begins by examining its own server and discovers the names of other servers. It then queries each of these servers to discover more servers and repeats this process until no more servers are found.

In addition, NXPIPX reads the connection table of each NetWare server to determine which NetWare clients are logged in to the server. NXPIPX sends IPX diagnostic packets to each client to collect additional information. Any clients that do not appear in the connection table because they have not been logged in recently are not discovered by NXPIPX. Any clients that have IPX diagnostics turned off are not discovered by NXPIPX. Therefore, it is important to schedule discovery to run when most clients are logged in. It is also important to leave IPX diagnostics enabled on NetWare clients. NXPIPX also discovers IPX routers in your network. Third-party IPX routers are discovered only if there is a NetWare server on the routed segment. NXPIPX does not discover interface information when routed segments do not have NetWare servers.

By default, NXPIPX attempts to discover your entire IPX internetwork. You can restrict the scope of discovery by specifying a list of IPX network numbers using NXPCON. Note that one of the IPX numbers must be bound to the NetExplorer Server for NXPIPX to discover other IPX nodes.


NXPLANZ

NetWare LANalyzer Agent monitors every packet on the network segment it is installed on, creating a list in local memory of all the physical (MAC) addresses and IP addresses of all the systems communicating on the segment. After NXPIPX completes its first pass, NXPLANZ uses SNMP to query all NetWare LANalyzer Agent servers and LANtern network monitors to read the list of workstations they have observed communicating on the network. NXPLANZ obtains a

list of NetWare LANalyzer Agent servers from NXPIPX. The addresses of LANtern monitors are not discovered automatically. Therefore, you should enter these addresses using NXPCON. You do not need to enter the address of a LANtern agent if you have NetWare LANalyzer Agent on the same segment.

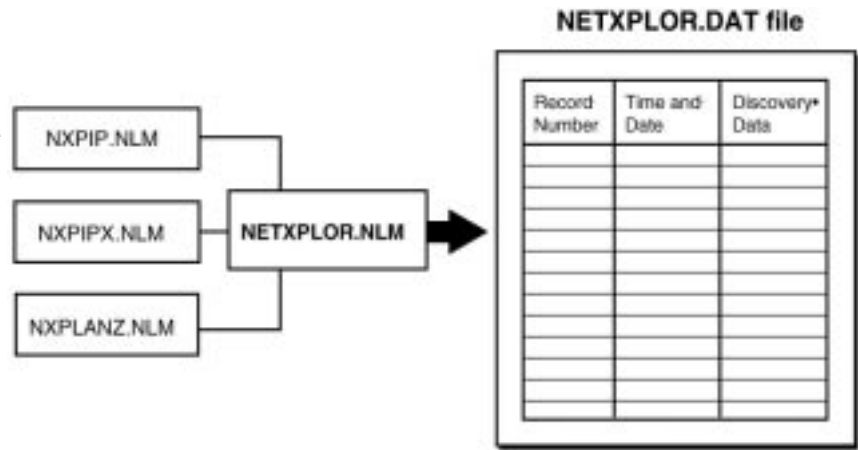
NETXPLOD

As the discovery processes gather information about systems on the network, they forward records of related data to NETXPLOD.NLM. NETXPLOD.NLM places these packets, along with a record number and a time stamp, into the NETXPLOD.DAT file, as shown in Figure G-5.

Note

ManageWise re-creates the NETXPLOD.DAT file each time you load NETXPLOD.NLM. Therefore, the discovery data stored at the NetExplorer Server from previous runs of the NetExplorer NLM processes is not retained when you restart NETXPLOD.NLM.

Figure G-5
NetExplorer
Discovery and the
NETXPLOD.DAT File



SNMP Community Name Discovery

Each time NetExplorer tries to access a system using SNMP, it uses the community names that have been configured using the NXPCON utility on the NetExplorer Server. When it encounters a new system, it tries each of the configured community names, in turn, until it finds one that results in a successful response. After it has found a community

name for a particular IP or IPX address, it records this name in a file so that in subsequent cycles, it does not need to retry with the other configured names. You can view these community names using NXPCON. The community names are used in the order specified. Therefore, the most-used community name should be configured first in the list.

Note



An SNMP query with an invalid SNMP community name results in no response from the target system; the request just times out.

NetExplorer Manager

NetExplorer Manager resides on each of the ManageWise Consoles and performs the following tasks:

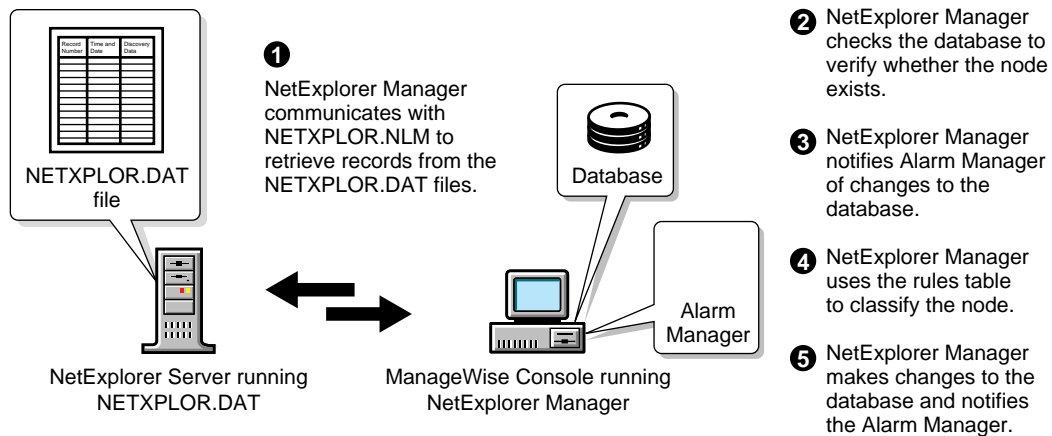
- ◆ Communicates with NETXPLOE.NLM to retrieve records from the NETXPLOE.DAT file
- ◆ Interprets these records
- ◆ Checks to see whether the system has already been discovered
- ◆ Uses a set of rules to determine any additional attributes of the discovered system
- ◆ Generates NetExplorer alarms
- ◆ Writes discovery information to the ManageWise database

Figure G-6 shows the operation of NetExplorer Manager. NetExplorer Manager begins by establishing a connection to the NetExplorer Server. NETXPLOE.NLM then starts reading records from the NETXPLOE.DAT file and sends the records to NetExplorer Manager. NetExplorer Manager remembers the record number of the last record processed. If NetExplorer Manager stops due to scheduling, or if the connection is broken between NetExplorer Manager and the NetExplorer Server, NetExplorer Manager requests records from the point where it left off when it reconnects to the NetExplorer Server. However, if the NLM processes are restarted, the NETXPLOE.DAT file is re-created and NetExplorer Manager requests the first record in the new file.

When NetExplorer Manager retrieves a record from the NetExplorer Server, it searches the database to determine whether the system

referred to by the record is in the database. If the system is not in the database, NetExplorer Manager inserts it. When NetExplorer Manager updates the database, it notifies Alarm Manager of the change. Alarm Manager records the change in the Alarm Report and marks maps as “Changed” in their window titles.

Figure G-6
NetExplorer Manager



NetExplorer Manager then looks for a rule in its rules table to help classify the system. The rules help NetExplorer Manager make decisions, such as which icon should be used to display the system on the maps. If the system in the record matches one of the rules, NetExplorer Manager updates the database according to the rule.

NetExplorer Manager first applies rules that are permanently built in to ManageWise, and then applies rules that have been added by applications that “snap in” to ManageWise, such as third-party applications.

Third-party rules are added to the NetExplorer Rules table by third-party ManageWise applications to enhance NetExplorer discovery. The ManageWise Software Development Kit (SDK) provides a tool for editing rules. Refer to *ManageWise SDK Overview* for more information.

MAC address rules define additional attributes for network objects within a MAC address range. For example, a built-in MAC address rule

specifies that a MAC address with a prefix of 00-00-1B is a Novell® network adapter. ManageWise predefines a large number of MAC address rules.

Systems for which very few, or no, rules apply have the Unknown system icon. If you install third-party applications that update the rules after NetExplorer Manager has run, these new rules do not affect the database unless you restart the NetExplorer NLM processes. This causes NetExplorer Manager to reprocess records for all systems on the network.

Names of Discovered Objects

ManageWise displays the names of discovered systems in maps, tables, and dialog boxes.

Naming is a complex process. As discovery cycles proceed and more information arrives, the names displayed in ManageWise maps and other windows can change. Also, ManageWise gives different priorities to names, depending on the source of the name information.

This section provides information about the priority of name sources and some general statements about names displayed in maps, tables, and dialog boxes.

Name Source Priority

This information applies to the *final* name displayed after discovery is complete. The various sources of name information and their priorities are shown in Table G-2.

Table G-2
Name Source Priorities

Source	Priority	Comments
User	1	Names you enter in the database take precedence over discovered names. NetExplorer Manager never changes a name you enter.
Bindery	2	
Server name		IPX server names are located in the server AUTOEXEC.NCF file; ManageWise obtains them from the bindery.
User name		Logged in or attached usernames are retrieved from NetWare Management Agent.
Service name		Service names are located in the bindery; systems send them in SAP packets.
MIB-II	2	If you do not configure the name in the MIB, NXPIP assigns a name of NONAME.
NetWare Management Agent	2	Discovered through NXPIP.
Names created by ManageWise	3	If NetExplorer cannot find any other name, it creates a name using the MAC address of the system.

General Information about Naming

The following are not rules, but general statements that might help you understand the names ManageWise displays:

- ◆ NetExplorer never changes names of systems you enter.
- ◆ Names shown in ManageWise maps and other windows are sensitive to discovery order.

- ◆ Name of a workstation logged in to multiple servers under different usernames can alternate (“flip-flop”) between the different usernames if you restart NETXPLOE.NLM.

Location Unknown Segment

Most systems that ManageWise discovers are placed immediately on the correct segment. However, if too little information arrives to identify a system, it appears in a special segment called LOCATION UNKNOWN. This segment contains certain partially discovered systems.

In some cases, ManageWise places systems in the LOCATION UNKNOWN segment during the early discovery processes of the initial discovery cycle and relocates them to their correct segment when a later process provides additional information. For example, when a router is configured to filter IPX diagnostic packets, any IPX system on the other side of the router is placed in the LOCATION UNKNOWN segment.

ManageWise moves the systems from the LOCATION UNKNOWN segment to the correct segment if an IP or IPX address is discovered.

You can move these systems to the correct segment by configuring them with the appropriate network address information. For more information about the LOCATION UNKNOWN segment, refer to the chapter on troubleshooting in *ManageWise 2.6 Network Management Guide*.

What NetExplorer Discovers

NXPIP, NXPIPX, and NXPLANZ use a variety of techniques to discover the following categories of network objects and present them on the ManageWise maps:

- ◆ Systems
- ◆ Network segments

In most instances, information gathered by NXPIP and NXPIPX is sufficient to place systems on the network maps correctly. However, when NXPIP and NXPIPX do not gather enough information, NXPLANZ retrieves MAC addresses collected by the NetWare

LANalyzer Agent software and LANtern network monitors. If NXPIP and NXPIPX have not discovered systems using these MAC addresses, the new systems are added to the database. Consequently, all systems are discovered on segments monitored by NetWare LANalyzer Agent or LANtern network monitor.

The following sections discuss details concerning the information that ManageWise discovers within each of these categories.

Systems Discovered by NetExplorer

Table G-3 shows the types of systems in the network the NetExplorer NLM files discover.

Table G-3
Systems Discovered by NetExplorer

System	Comment
NetWare File Server	Service type of 4 (File Server)
IPX Router	System with more than one adapter connected to different IPX networks
IP Router	System that is configured as an IP router in MIB-II (IP Forwarding enabled)
NetWare Print Server	Service type of 71 or 7 decimal
NetWare Client™ Workstation	System that responds to IPX diagnostics requests as an IPX workstation (has the NetWare Shell loaded)
HMI Hub Service	Service type of 569 decimal
LANtern Network Monitor	User enters information using NXPCON
SFT III IO Engine	Discovered by IPX discovery module; responds with diagnostic information
SFT III MS Engine	Discovered by IPX discovery module
UnixWare* Workstation	Service type of 996 decimal
NetWare Management Agent	Service type of 563 decimal (NetWare Management Agent 1.5 or 1.6) or 635 decimal (NetWare Management Agent 2.6)
NetWare LANalyzer Agent	Service type of 570 decimal
Network Printers	Discovered if the printer generates a well-known service type
NetWare Connect™ Server	Service type of 590 decimal
NetWare Communications Server	Used by the NetWare for SAA* services manager products; has a service type of 304 decimal
NetExplorer Server	Running NetExplorer discovery NLM files; has a service type of 567 decimal
Any System	Any system is discovered if it is connected to a LAN segment being monitored by NetWare LANalyzer Agent

NetWare Servers

NXPIPX discovers all NetWare servers from the NetWare 2 family, NetWare 3 family, NetWare 4 family, and later.


NetWare Client Workstations

NXPIPX discovers all NetWare clients attached to discovered NetWare 3, NetWare 4, and later servers. Clients that are turned off or not attached to any server are not discovered. For this reason, a NetExplorer pass run at night or on a weekend might not yield a complete map. Note that NetWare clients must have IPX diagnostics enabled.

When you configure a NetWare client to perform a bindery login, consider the scenarios in Table G-4.

Table G-4
Configuration Scenarios for Bindery Login

Server	Bindery Login—What Is Discovered
NetWare 3, NetWare 4 or NetWare 5 with NetWare Management Agent installed	Workstation discovered; name discovered only if logged in
NetWare 3 with NXPPLUS	Workstation discovered; name discovered only if logged in
NetWare 3, NetWare 4 or NetWare 5	Workstation discovered; name not discovered

Note

NXPPLUS.NLM became obsolete with NetWare Management Agent 2.6. However, if NetExplorer finds NXPPLUS on a server not running NetWare Management Agent 2.6, NetExplorer uses it.

When you configure the client to perform a directory login, NetExplorer discovers the system only when it is logged in to an NDS tree. NetExplorer does not discover the system when it is just attached to the NDS tree. NXPIPX uses SNMP to query NetWare Management Agent on all NetWare servers for the username. To communicate with NetWare Management Agent, NetExplorer must have knowledge of the SNMP community name.

After NetExplorer discovers a NetWare client, NXPIPX queries it using the IPX diagnostic protocol to confirm the discovery and gather more

information about it. If IPX diagnostics are turned off, NXPIP does not report the system. This applies to printers as well.

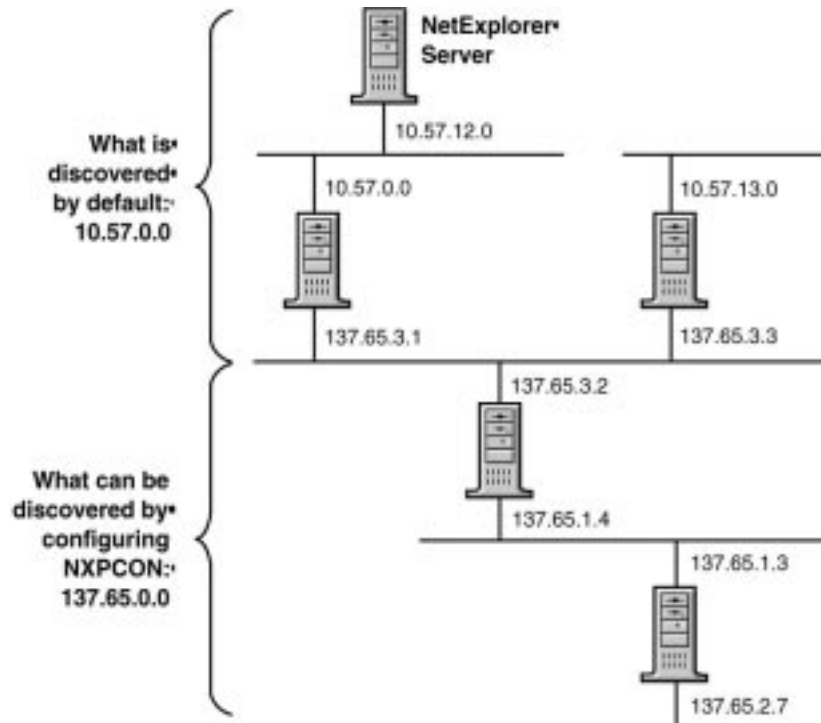
IP Routers

NXPIP uses SNMP to query all IP routers on the network. To communicate with a router, NetExplorer must have knowledge of the SNMP community name it uses. You must enter the list of community names used by your routers using NXPCON. NXPIP does not discover routers using community names that are not listed in NXPCON.

If you configure router information such as the system name and location in the router's SNMP Management Information Base (MIB), ManageWise records it in the database, allowing IP routers to be displayed on maps with a meaningful name. You can configure this information into the router's MIB using any SNMP configuration tool, including the ManageWise SNMP MIB Browser.

By default, IP discovery discovers only the same network number as the NetExplorer Server (seen in Figure G-7). For example, if the NetExplorer Server IP address is 10.57.12.0, the IP discovery NLM discovers the entire 10.57.0.0 network and its subnets. Note that the segment that it is on is also discovered. The exploration can be expanded by specifying additional network numbers using the NXPCON *Discovery Scope > IP Discovery Scope* command. Also, if there are redundant IP routers, use the NXPCON *IP Discovery > IP Routers* command to specify the redundant IP router address; otherwise NXPIP does not discover it.

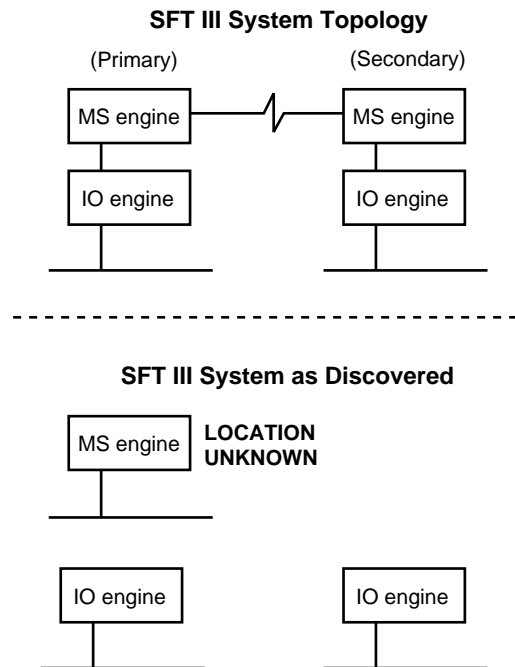
**Figure G-7
IP Router
Discovery**



NetWare SFT III Servers

A NetWare SFT III (System Fault Tolerant) server consists of two systems, each containing an IO engine and an MS engine (mirror server). NetExplorer fully discovers each IO engine and places it on the correct segment. Because the two MS engines implement only one logical server on the network and its location can change depending on which copy is the primary, NetExplorer places it on the LOCATION UNKNOWN segment. Figure G-8 illustrates this.

Figure G-8
NetWare SFT III
Server Discovery



When the MS engine does not have NetWare Management Agent loaded, NetExplorer discovers only the MS engine and the primary IO engine. NetExplorer does not discover the secondary IO engine; the primary IO engine appears with the name "NONAME."

When NetWare Management Agent is loaded, the MS engine and both of the IO engines are discovered correctly with their names. Double-clicking any engine on the map brings up the system schematic, which shows the other engines of the server.

Systems Monitored by NetWare LANalyzer Agent

NetExplorer discovers all systems communicating on segments monitored by NetWare LANalyzer Agent. For information about NetWare LANalyzer Agent servers, refer to "NetWare LANalyzer Agent Servers" on page 137.

Systems Not Equipped with the IPX Diagnostic Responder

NXPIPX discovers the following systems but does not necessarily place them correctly on the ManageWise maps:

- ◆ NetWare for UNIX® servers
- ◆ Portable NetWare servers
- ◆ Access servers
- ◆ Modem servers
- ◆ Print servers

Because these systems do not respond to IPX diagnostics, they cannot answer queries from NXPIPX. Consequently, the LAN information required to place them on the maps might not be available. In this situation, NetExplorer places these systems in the LOCATION UNKNOWN segment map. In most cases, the presence of NetWare LANalyzer Agent on each segment that these systems appear on enables NetExplorer to obtain the missing information and correctly locate the systems in the maps. You can move systems in LOCATION UNKNOWN manually to the correct segment by using *Edit > Database Object* from the ManageWise Console.

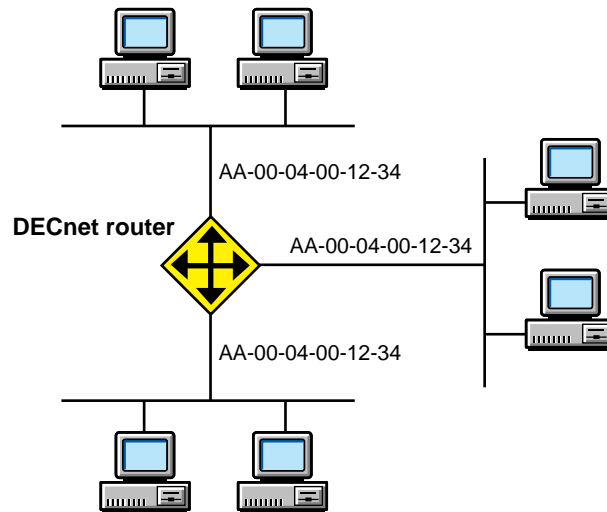
Routers That Use Duplicate MAC Addresses

NetExplorer can experience difficulties correctly discovering some routers because of the method the routers use to identify their adapters. In some cases, the same MAC address is used on several network interfaces of a router. In these cases, it appears to NetExplorer that one adapter is connected to multiple segments. Unless otherwise specified, NetExplorer interprets that the multiple adapters are one adapter.

Therefore, the multiple segments that the adapters are connected to are seen as one segment and NetExplorer mistakenly consolidates the multiple segments. You can set special rules in the NetExplorer section of the NMS.INI file to describe these conditions. Rules for DECnet* addressing and Bay Networks routers, two cases where duplicate addresses are used, are placed in the NMS.INI file at installation.

For example, ManageWise has a special rule to determine when DECnet routing is in use. Figure G-9 shows an example of a DECnet router that has three interfaces with the same MAC address (AA-00-04-00-12-34).

Figure G-9
DECnet Router
Example



In the NetExplorer section of the NMS.INI file, AA-00-04 is designated as a duplicate MAC address (DupMac1=AA0004). This tells NetExplorer Manager that any MAC address beginning with AA-00-04 can be duplicated. Therefore, NetExplorer Manager knows not to treat the address as unique. A similar rule in the NMS.INI file exists for Bay Networks routers. You can make additions to the NMS.INI file for other router types. If your network routes the XNS* protocol, you must enter the MAC address of the routers in the NMS.INI file. Rules to define duplicate MAC addresses can also be used for ARCNET* systems, NetWare Connect servers, and servers running DOSBOX.NLM. These systems have non-unique MAC addresses. Refer to the chapter on troubleshooting in the *ManageWise 2.6 Network Management Guide* for more information.

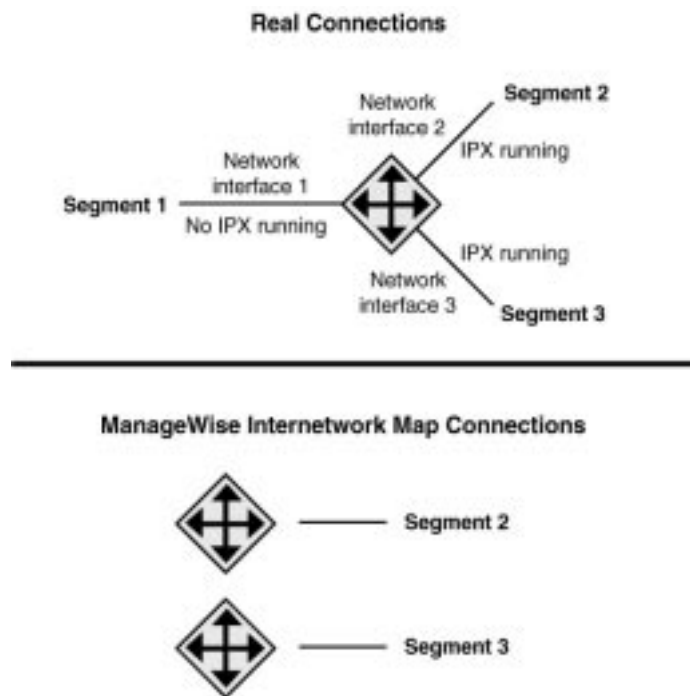
Third-Party Routers

NXPIP discovers IP-bound interfaces only. In a case where IP is not being run on a router, NetExplorer discovers the IPX-bound interfaces resulting with the following on the maps:

- ◆ A separate router icon is shown for each interface in the router.
- ◆ Interfaces that are discovered are not placed in the same router on the ManageWise maps. Consequently, the interconnections are not correct on the internetwork map and the router appears as multiple, separate routers, each containing one network interface from the real router.

Figure G-10 illustrates a router with IPX running on Network Interfaces 2 and 3 but not on Network Interface 1. NetExplorer would mistakenly place this router on the internetwork map as two separate systems. As shown, the connection to Segment 1 is not displayed, and the connections to Segments 2 and 3 are shown attached to two separate systems. Refer to the chapter on troubleshooting in the *ManageWise 2.6 Network Management Guide* for more information.

Figure G-10
Third-Party Router
Example



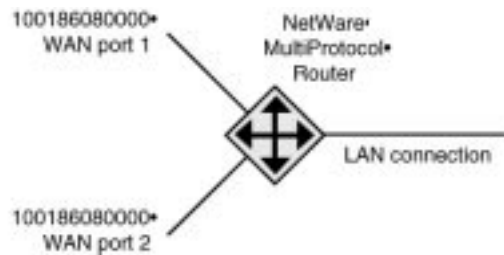
NetWare MultiProtocol Router with WAN Ports

In some cases, NetExplorer has difficulty discovering NetWare MultiProtocol Router™ WAN interfaces correctly. The accuracy of discovery depends on which version of the software you are running.

NetWare MultiProtocol Router 2.0 and 2.1

Figure G-11 demonstrates NetWare MultiProtocol Router 2.0 or 2.1 with two WAN ports.

Figure G-11
NetWare
MultiProtocol
Router Example



The NetWare MultiProtocol Router software assigns the network addresses of WAN Ports 1 and 2 using the internal network number of the router and adding zeros. This results in an address for both WAN Port 1 and WAN Port 2 of 100186080000. To prevent NetExplorer Manager from consolidating both of these ports as a single port, you must enter the address of the WAN connection in the NetExplorer section of the NMS.INI file as a duplicate address. Also, NetWare MultiProtocol Router 2.0 and 2.1 do not return the correct segment type for WAN links, resulting in an incorrect icon being placed on the internetwork map, with a status of UNKNOWN. This applies to both IP and IPX discovery.

NetWare MultiProtocol Router 3.0

If you are running NetWare MultiProtocol Router 3.0, the following sections apply.

IPX Discovery

NetWare MultiProtocol Router 3.0 correctly reports the segment type of WAN links. NetExplorer detects these correctly and displays them with the appropriate icon.

IPX WAN links between NetWare MultiProtocol Router 3.0 systems do not have an IPX network associated with the link. When NetExplorer discovers such a link, it creates a name for the WAN segment of the form #UNNUM-*n*, where *n* is an integer assigned to make the segment name unique. On multiaccess networks such as frame relay and X.25, each connection in the network adds another #UNNUM-*n* to the segment name.

IP Discovery

With NetWare MultiProtocol Router 3.0, you can configure both numbered and unnumbered IP links. NetExplorer discovers numbered links correctly. NetExplorer does not discover unnumbered IP links, resulting in an island (the link is missing) appearing on the map. Select the *Edit > Connect Objects* command in the ManageWise Console to connect a router to a segment to join the islands.

If IP is running on a third-party router and NXPIP is running on the NetExplorer Server, NetExplorer discovers only the IP-bound interfaces. The router is shown correctly on the ManageWise maps. If IP is not running on a third-party router but NXPIPX is running on the NetExplorer Server, NetExplorer discovers the IPX-bound interfaces. However, these IPX-bound interfaces are not placed in the same router icon on the ManageWise maps.

On-Demand Links

An on-demand link is a WAN connection between two routers in which only user data (no routing traffic) is exchanged across the link. The link is brought up “on-demand”; that is, only when there is data to send.

NetExplorer discovers on-demand IP and IPX links correctly if sufficient static routing information has been configured to allow the NetExplorer server to reach the other side of the on-demand link.

However, if a link is an on-demand and unnumbered IP link, the entire topology on the remote end of the link is not discovered. Use the *IP*

Discovery > Additional IP Routers command of the NXPCON utility to configure an additional IP router address for the “missing” router.

Third-Party Routers with WAN Ports

NetExplorer discovers third-party routers correctly if they support MIB-II SNMP. Certain third-party routers can have a WAN link with no IP or IPX network number on the link itself. In this case, the WAN link is not discovered. Use the ManageWise map editing feature to add a new WAN segment and to connect the routers to this segment.

NetWare Connect Servers

NetExplorer discovers NetWare Connect servers, but if you have more than one NetWare Connect server on the network, NetExplorer consolidates them and they appear as one server. To properly identify them, you need to specify a duplicate MAC address entry in the NMS.INI file.

Refer to the chapter on troubleshooting in the *ManageWise 2.6 Network Management Guide* for additional information.

Network Segments Discovered by NetExplorer

NetExplorer discovers the following network segments:

- ◆ LAN and WAN segment types
- ◆ Source-route bridged token rings

LAN and WAN Segment Types

NetExplorer discovers the following LAN and WAN segment types:

- ◆ ATM
- ◆ LAN: ARCNET
- ◆ LAN: FDDI
- ◆ LAN: Ethernet
- ◆ LAN: LocalTalk*

- ◆ LAN: Token Ring
- ◆ SMDS
- ◆ WAN: X.25
- ◆ WAN: ISDN
- ◆ WAN: SDLC
- ◆ WAN: Serial
- ◆ WAN: PPP
- ◆ WAN: Frame_Relay
- ◆ WAN: T1
- ◆ WAN: T3

These values are discovered correctly if a system connected to the segment responds with an interface type from MIB-II RFC 1573.

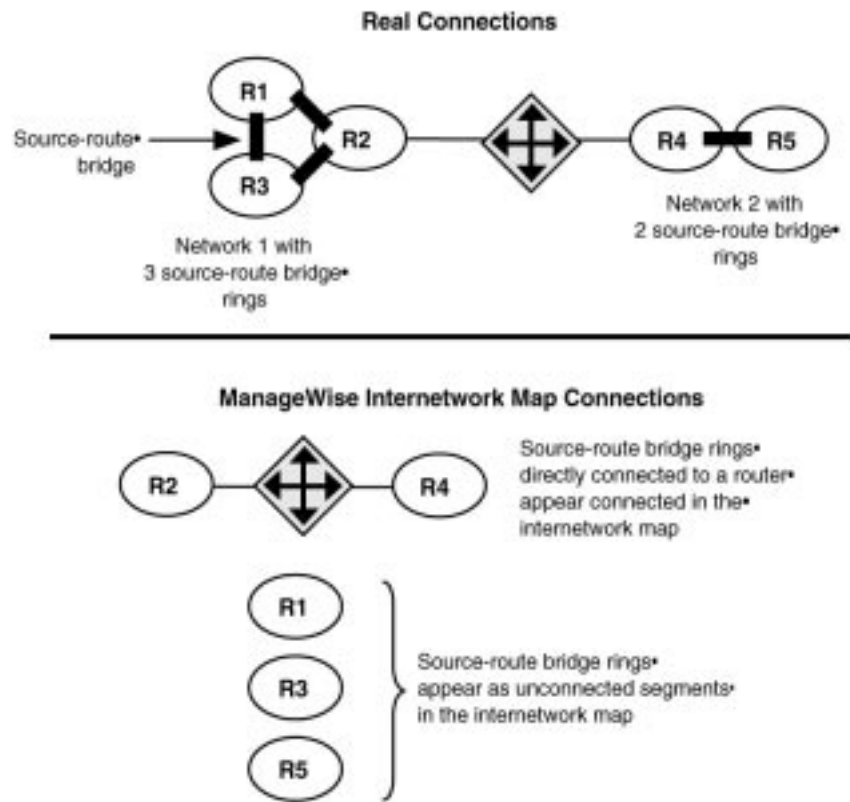
Source-Route Bridged Token Rings

The way ManageWise maps display source-route bridged token rings depends on whether you have NetWare LANalyzer Agent installed on each ring:

- ◆ If you do *not* have NetWare LANalyzer Agent installed on each source-route bridged token ring in your network, ManageWise discovers the network but consolidates all source-route bridged token rings that share the same IPX network number or IP subnet into a single segment. For example, in Figure G-12, rings R1, R2, and R3 are displayed as one segment, and rings R4 and R5 are displayed as another segment on the internetwork map.
- ◆ If you *do* have NetWare LANalyzer Agent installed on each source-route bridged token ring, each NetWare LANalyzer Agent discovers its own ring (segment) and every system on it. ManageWise displays the ring as an unconnected segment on the internetwork map.

- ◆ If you have NetWare LANalyzer Agent installed on a source-route bridged token ring connected to a router, the ManageWise internetwork map shows the correct connections. However, if two networks each have several rings and only one ring in each network is connected to a router, the ManageWise internetwork map shows the correct connections only of the rings that are *directly* connected to the router. The other source-route bridged token rings in each network are displayed as disconnected segments on the internetwork map. Figure G-12 illustrates this second case.

Figure G-12
Source-Route
Bridge, as Shown
on the ManageWise
Internetwork Map



In all cases, bridge information is not discovered. As a consequence, NetExplorer treats each interface of a source-route bridge as a separate

system on the network. One icon appears on the ManageWise maps for each interface of the source-route bridge.

When you have NetWare LANalyzer Agent installed on one server on each ring of an IPX source-route bridged network, the segment names displayed on the ManageWise internetwork map consist of the IPX network number followed by the MAC address of that server's interface to the ring. If NetWare LANalyzer Agent is monitoring more than one interface, the address shown for a ring is the MAC address of the interface monitoring that ring.

You can correct all these problems manually by creating bridges and rings using the Edit function of the ManageWise Console. After you create the bridges and token ring segments and move the token ring systems to the correct segments, NetExplorer does not undo your changes. We recommend that you make changes after NetExplorer Manager has finished processing first-cycle records from NETXPLOER.NLM. Refer to the chapter on troubleshooting in *ManageWise 2.6 Network Management Guide*.

Transparent Bridges

NetExplorer cannot fully discover transparent bridges. ManageWise consolidates groups of transparently bridged segments running the same network number into a single segment on the maps. You can correct this problem by using the *Edit > Add* command in the ManageWise Console to create the segments and bridges that are not discovered, and then move discovered systems to the correct segment.

Configuration Changes

NetExplorer detects most changes in the network topology, such as the addition, reconfiguration, or deletion of interfaces, resulting in changes being made to the internetwork maps. However, if you remove the system from the network, it is not detected unless you move it to another location in the network. You can delete systems manually from any of the ManageWise maps.

Load Considerations for Running NetExplorer

To help you plan the impact that NetExplorer will have on your network, data from discovery sessions involving the following two sample networks is provided:

- ◆ A 28-node network
- ◆ A 6530-node internetwork

The following equipment was used to operate NetExplorer in these sample discovery sessions:

- ◆ The NetExplorer Server was an AST* 486/66 with 40 MB of RAM, running only the NLM files required for NetExplorer.
- ◆ The ManageWise Console was an AST 486/66 with 16 MB of RAM, running only the ManageWise Console software.

These examples provide load statistics for the ManageWise Console, the NetExplorer Server, and the network that is being discovered. Table G-5 describes each of the statistics obtained in the tests.

Table G-5
Key to Test Statistics

Test Statistic	Description
Average Network Utilization	Describes the average percent network utilization during the course of the cycle being tested. This statistic is an average: utilization spikes up to a higher percentage for periods of time during operation.
Average CPU Utilization	Describes the average percent CPU utilization of the NetExplorer Server during the course of the cycle being tested. This statistic is an average: utilization spikes up to a higher percentage for periods of time during operation.
Memory (RAM) Used	Indicates the amount of RAM used by the discovery process during specific operations of the test. Statistics are given for memory used during discovery and data transmission to the ManageWise Console.
Average Packet Rate	Indicates the average number of packets, in packets per second, on the affected network during the discovery cycle and while the NetExplorer Server is transmitting to the ManageWise Console.

Table G-6 describes the network configurations used for the tests.

Table G-6
Network Configurations Used for Tests

Network Configurations	Description
High Speed WAN Link (1.536 Mbps)	Indicates what the load on a fast remote link would be if the entire network being discovered were on the other side of the remote link from the NetExplorer Server. During discovery, the ManageWise Console was continuously receiving data from the NetExplorer Server.
Slow Speed WAN Link (56 Kbps)	Indicates what the load on a slow remote link would be if the entire network being discovered were on the other side of the remote link from the NetExplorer Server. During discovery, the ManageWise Console was continuously receiving data from the NetExplorer Server.
Ethernet LAN	Indicates what the load on an Ethernet LAN would be during discovery. During discovery, the ManageWise Console was continuously receiving data from the NetExplorer Server.

28-Node Network Example

In this example, a network with 28 nodes was discovered so that the impact of discovery on the NetExplorer Server, the network being discovered, and the ManageWise Console could be measured. As clearly demonstrated by the statistics, the impact of operating the NetExplorer discovery NLM software was minimal on network, server, and remote link performance. Table G-7 provides a brief description of these performance impacts.

Table G-7
Summary of Test Results from 28-Node Example

NetExplorer Component	Performance Impact while Running NetExplorer
NetExplorer Server	When you load NetExplorer, you need 3 MB of RAM to discover a small network. This is beyond your base RAM server requirements.
Network Being Discovered Over a LAN	Minimal increase in average CPU utilization (14%) was shown during operation of NetExplorer. Minimal increase of 10 packets per second was added to the average packet rate during operation of NetExplorer for both discovery and transmission to the ManageWise Console. Average utilization of the Ethernet LAN is typically less than 1% of total bandwidth.

Table G-7 *continued***Summary of Test Results from 28-Node Example**

NetExplorer Component	Performance Impact while Running NetExplorer
Fast Remote Link	Minimal increase of 13 packets per second was added to the average packet rate during operation of NetExplorer for both discovery and transmission to the ManageWise Console. Average utilization of the link is typically less than 1% of total bandwidth.
Slow Remote Link	Minimal increase of 10 packets per second was added to the average packet rate during operation of NetExplorer for both discovery and transmission to the ManageWise Console. Average utilization of the link is typically 1% of total bandwidth.
ManageWise Console	During the initial discovery cycle, when the ManageWise maps were being created, ManageWise Console performance was impacted significantly. However, during subsequent discovery cycles, the ManageWise Console experienced only occasional periods when performance was noticeably affected.

6530-Node Internetwork Example

In this example, an internetwork with 6530 nodes was discovered so that the impact of discovery on the NetExplorer Server, the network being discovered, and the ManageWise Console could be measured. As clearly demonstrated by the statistics, the impact of operating NetExplorer was minimal on network, server, and remote link performance. Table G-8 provides a brief description of these performance impacts.

Table G-8

Summary of Test Results from 6530-Node Example

NetExplorer Component	Performance Impact while Running NetExplorer
NetExplorer Server	When you load NetExplorer, you need 8 MB of RAM to discover a large network. This is beyond your base RAM server requirements.
Network Being Discovered Over a LAN	Minimal increase in average CPU utilization (13%) was shown during operation of NetExplorer. Minimal increase of 27 packets per second was added to the average packet rate during operation of NetExplorer for both discovery and transmission to the ManageWise Console. Average utilization of the Ethernet LAN is typically less than 1% of total bandwidth.

Table G-8 *continued*

Summary of Test Results from 6530-Node Example

NetExplorer Component	Performance Impact while Running NetExplorer
Fast Remote Link	Minimal increase of 33 packets per second was added to the average packet rate during operation of NetExplorer for both discovery and transmission to the ManageWise Console. Average utilization of the link is typically less than 1% of total bandwidth.
Slow Remote Link	Minimal increase of 27 packets per second was added to the average packet rate during operation of NetExplorer for both discovery and transmission to the ManageWise Console. Average utilization of the link is typically 1% of total bandwidth.
ManageWise Console	During the initial discovery cycle, when the ManageWise maps were being created, ManageWise Console performance was impacted significantly. However, during subsequent discovery cycles, the ManageWise Console experienced only occasional periods when performance was impacted to a noticeable extent.

appendix **H** ***Multiple ManageWise Servers in One NDS Container***

This appendix describes some options for how you might want to set up your NDS environment to work with ManageWise® software.

When you install ManageWise Servers on your network, you can be confronted with many configuration strategies. For example, in a container, do you want one server to manage all the functions of ManageWise (network discovery, workstation inventory scan, and virus scan), or do you want one server to discover your network and another to perform workstation inventory scan and virus scan functions? The following are some setup strategies. The first management strategy is easiest; the second is more complex.

1. Select one of the ManageWise Servers as the server to perform all ManageWise functions and make it the default server for every user in the container. Use this strategy for containers that have nodes that are physically close to one another and do not have a large number of users.
2. For a container in which you divided the functions (network discovery and so on, on one server and workstation inventory and virus scan on another), split the container so that there is only one ManageWise Server performing workstation inventory and virus scan per container. This is labor intensive and should be considered only if your network is very large and you are splitting the container anyway.

Index

A

- Adding users to ManageWise user group 19
- Address masks
 - specifying for IP 49
 - specifying for IPX 50
- Agent, description 6
- Alarm disposition 69
- Alarm thresholds
 - adjusting 70
- Alarms
 - adjusting thresholds 70
 - enabling for segments 69
 - sending to third-party management stations 76
 - token ring 92
- AMSAPI.NLM file 27
- Anti-virus protection 59, 102
- AppleTalk objects, discovery of 48
- Autodiscovery. *See* Discovery
- AUTOEXEC.NCF file 94, 116, 117, 124

B

- Baseline documents 71
- Bridges
 - token ring 160
 - transparent 162
- BSTART.NCF file, caution against using 97
- Btrieve
 - environment troubleshooting 97 to ??
 - errors 1002 and 2001 106
 - parameters 97

C

- Changing network interface cards 93
- Chat, editing security template 65
- Checklists, third-party application information log 86
- Client configuration utility 101
 - running manually 101
- CLNTCFG.EXE file 101
 - running manually 101
- Community names
 - configuring 47
 - discovery 142
- Components, ManageWise 2
- Configuring
 - DOS Clients 28
 - ManageWise clients 101
 - NDS environments 167
 - network object discovery 14
 - SNMP community names 47
 - Win3.x/95 Clients 29
 - Windows NT Clients 32
- CONLOG.NLM file, use in reviewing NLM
 - loading 94, 109, 110
- Continuous discovery 139
- Creating a Macintosh Install Diskette 62
- Custom maps 14
 - creating 71

D

- Default security template, editing 65
- Desktop Management troubleshooting

- server control 101
- Desktop Remote
 - changes to SYSTEM.INI file 129
 - files installed 129
 - installing 80
 - modem communications 80
 - system requirements 80
 - use of 79 to 129
 - VUSER.386 file 129
 - workstation changes 129
- Discovered objects 6
- Discovery
 - configuring 14
 - scope of 48, 51
 - continuous 139
 - cycle 139
 - initial cycle 41, 42
 - IP 158
 - IP routers 151
 - IPX 158
 - names assigned to objects 145
 - NetExplorer Manager 143
 - NetWare Client workstations 150
 - NetWare servers 150
 - network topology 39
 - NETXPLORE 142
 - NLM file memory requirements for 91
 - NXPIP 140
 - NXPIPX 141
 - NXPLANZ 141
 - object names 145
 - of AppleTalk objects 48
 - of IPX objects 48
 - of Macintosh objects 48
 - on-demand links 158
 - process 6, 39, 131, 139
 - reviewing maps after 68
 - scheduled 140
 - SFT III servers 152
 - starting 41, 42
 - status checking 43, 44
 - systems 149
- Discovery cycle
 - overview 139

- timing sequence 139, 140
- Disposition of alarms 69

E

- Error messages
 - Agent Not Monitoring 105
 - Btrieve MACHINES.DAT 107
 - Btrieve TYPES.DAT 107
 - Btrieve VALUES.DAT 107
 - Btrieve, numbered 1002 or 2001 106
 - Communication with server failed (Error 251) 107
 - Error LANS001 Invalid temporary path 108
 - Instrumented OS Emulator unable to Register
 - Object class 108
 - Module NETXPLORE.NLM not loaded 108
 - No resources on probe 109
 - No response 110
 - Out of top N resources 110
 - Unable to access default security parameters 111
 - Unable to copy files 90
 - Unable to read user's Access Rights List on
 - server 111
 - Wrong version of DLL CTL3D.DLL 112
 - You have no console privileges on this server 112

F

- File backups for server, caution 113
- File Transfer, editing security template 65

I

- InocuLAN for Macintosh 62
- InocuLAN Server, defined 7
- INOMAC.EXE 62
- Internetwork maps 14
- Inventory database, rebuilding 98 to ??

- Inventory MacScan
 - installing 38
- inventory scans
 - workstations 121
- IO engines 153
- IP
 - routers 151
- IP addresses, specifying 49
- IP discovery scope, configuring 48
- IPX diagnostic responder 154
- IPX discovery scope, configuring 50
- IPX network numbers, specifying 50
- IPX objects, discovery of 48

L

- LANZ.NCF file 117
- LDISCAN.EXE 121
- LDISCAN.EXE file 121
 - memory use 97
- LDISCAN.NLM file 27
- LDISCAN2.EXE 121
- LDISCNNT.EXE 121
- Load considerations, running NetExplorer 163
- Loading NetExplorer modules 54
- LOCATION UNKNOWN segment 147
- Logging in to ManageWise Console 65
- Login scripts 120

M

- MAC address
 - duplicate 154
 - rules 144
- Macintosh devices, discovery of 48
- Macintosh workstations, software installation 38
- Management workstation
 - changes to
 - SYSTEM.INI file 127
 - WIN.INI file 127
- ManageWise
 - agents 7

- client configuration 101
 - components 2, 137
 - concepts 6
 - exiting 10
 - extracting data from 15
 - functions 1
 - generating reports from 15
 - information, adding to OU Profile 20
 - status bar elements 11
 - updates, obtaining 103
 - workstations, troubleshooting 100
- ManageWise clients
 - Macintosh workstations, software installation 38
- ManageWise Console 2
 - defined 7
 - functions protected by password 64
 - logging in 65
 - troubleshooting 94 to ??
 - window elements 11
- ManageWise database, adding information to 72
- ManageWise Login script 121
- ManageWise Server
 - abends 89
 - configuration 115 to 125
 - defined 7
 - troubleshooting 89 to 90
- ManageWise Server memory
 - maximum Packet Receive Buffers 91
 - maximum Physical Receive Packet Size 91
- ManageWise Server memory configuration 91
- ManageWise third-party applications 83
 - migrating 18, 88
- MANAGEWISEGROUP, adding users to 19
- Managing clients
 - with Profile login scripts 21
- Maps
 - how systems represented in 134
 - reviewing after discovery 68
 - types of 14
- Maps, custom 71
- Masks, specifying for IP addressing 49
- Masks, specifying for IPX addressing 50
- MEMMGR.NLM 132

Modem communications in Desktop Remote 80
MS engine 153

N

Names

- assigned to discovered objects 145
- priority of sources 146
- sensitive to discovery order 146

NetExplorer

- components 131, 134
- configuring 45
- Console Utility, using 40
- defined 6, 7
- files, backup caution 113
- initial discovery 41, 42
- load considerations 163
- NLM files 131
- overview 131, 134
- starting 41, 42
- system architecture 133
- system components 131
- system status 44
- what it discovers 147

NetExplorer Manager 143

- changing schedule for 55
- changing settings 55
- closing manually 57
- configuring to run continually 68
- configuring to run daily 56, 68
- defined 6
- described 131, 133
- evaluating the schedule 68
- starting manually 57

NetExplorer Server

- defined 7
- loading modules 45
- NETXPLOD.DAT 142
- NXPIP.NLM 136
- NXPIP.NLM 137
- unloading modules 47, 54

NetExplorer, loading modules 54

NetWare 3.x system login scripts 120

NetWare Client workstations 150

NetWare Connect servers 159

NetWare LANalyzer Agent 9, 10

- bridged token ring 160
- features of 9
- file backup caution 113
- nodes monitored by 153
- servers 137
- statistics reliability 93
- troubleshooting 92 to 94

NetWare Management Agent 8, 9

- servers 138

NetWare MultiProtocol Router 157

NetWare server

- discovery 138, 150
- SFT III 152

Network Dashboard

- missing bar chart 93

Network interface cards

- changing or adding 93

Network numbers, specifying for IPX 50

Network object discovery

- configuring 14
- scope of 48, 51
- initial cycle 41, 42
- starting 41, 42

Network topology 131

Network topology map types 14

NETXPLOD.DAT 139

NETXPLOD.NCF file 117

NETXPLOD.NLM 131

NLM files

- AMSAPI 27

NMA.NCF file 117

NMSBASE.NCF file 91, 117

NTSTACFG.EXE 32

NWCALLS.DLL file

- CTL3D.DLL file 112

NXPCON, using 40

NXPCON.NLM 132

NXPIP.NLM 131, 136

NXPIP.NLM 131, 137

NXPLANZ.NLM 137

NXPPLUS 150

O

- Object names 145
- On-demand links, discovery 158
- OU login scripts, adding ManageWise information to 21
- OU Profile, adding ManageWise information to 20

P

- Packet Receive Buffers, setting maximum number 91
- Password
 - protecting ManageWiseConsole 64
 - setting up, on ManageWise Console 65
- Patch files, obtaining 103
- Physical Receive Packet Size, modifying maximum value 91
- POPUPTSR.EXE file 123
- Profile login scripts
 - adding Managewise information to 21
 - using to manage clients 21
- Profile login scripts, creating 21
- PUSHPOP.EXE file 120

R

- Remote system requirements 80
- Rights, granting user 20
- Routers
 - IP 151
 - MAC address 154
 - NetWare MultiProtocol Router 2.0 and 2.1 157
 - NetWare MultiProtocol Router 3.0 157
 - SAP IDs 134
 - third-party 156
 - third-party with WAN ports 159
- Rules, MAC address 144

S

- SAP IDs 134
- Security template, editing the default 65
- Segment
 - enabling alarms for 69
 - LOCATION UNKNOWN 147
- Segment maps 14
- Server abends, troubleshooting 89
- Server backups, caution 113
- Server configuration 115 to 125
 - AUTOEXEC.NCF 117
 - AUTOEXEC.NCF file 116
 - LANZ.NCF file 117
 - NETXPLOD.NCF file 117
 - NMA.NCF file 117
 - NMSBASE.NCF file 117
- Server, NetWare Connect 159
- Setting Options with Windows Client Configuration Program 31
- Setting up InocuLAN for NetWare Server Software 59
- Setup tasks
 - first days 63
 - first weeks 64
- SFT III servers 152
- Short-term memory allocation failures, troubleshooting 91
- SNMP
 - community names 142
 - configuring 47
 - load parameters in AUTOEXEC.NCF file 94
- SNMP community names 47
- SNMP load parameters 94
- STARTUP.NCF file, modifying 92
- Statistics inaccuracies from NetWare LANalyzer Agent 93
- Statistics, test 163, 165
- Status bar elements 11
- Subnet masks, specifying 49
- System
 - representation of 134
- SYSTEM.INI file 127

Desktop Remote changes to 129

T

- Technical support, requesting 102
- Time discrepancies, resolving 101
- Timing sequence 139, 140
- Token ring alarms, receiving 92
- Token ring, bridged 160
- Topology maps
 - creation 39
 - types of 14
- Topology, network 131
- Troubleshooting
 - Desktop Management server control 101
 - ManageWise Console 94 to ??
 - ManageWise Console, Windows environment 96
 - ManageWise Server 89 to 90
 - ManageWise workstations 100
 - NetWare LANalyzer Agent 92 to 94
 - wide-area network environment 102
- Trustee rights, assigning 22

U

- Unloading NetExplorer modules 54
- Updates, obtaining 102
- User login scripts
 - adding Desktop management information to 20
- USER.NLM file 27
- Users
 - adding to ManageWise group 19
 - granting rights to 20
- USERTSR.EXE file 122

V

- Virus pattern files, obtaining updates 102
- Virus protection 59, 102
- VUSER.386 file 129

W

- WAN environment troubleshooting 102
- WAN ports 157
- Wide-area network environment
 - troubleshooting 102
- WIN.INI file 127